НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
“КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
ІМЕНІ ІГОРЯ СІКОРСЬКОГО”
Теплоенергетичний факультет
Кафедра автоматизації теплоенергетичних процесів

«На правах рукопису»
УДК 681.515+004.056.53

«До захисту допущено»
В.о.завідувача кафедри

_____ / *В.А.Волощук*/
“____” _____ 2019 р.

Магістерська дисертація
на здобуття ступеня магістра

зі спеціальності ***151“Автоматизація та комп’ютерно-інтегровані технології”***

на тему: Автоматизація процесу горіння котлоагрегату на твердому паливі

Виконав: студент II курсу, групи ТА(ТО)-81мп
Яремчук Ірина Тарасівна _____
(прізвище ім’я, по батькові) (підпис)

Науковий керівник Ст.викладач Ю.Є.Грудзинський _____
(посада, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Консультант _____ _____
(назва розділу) (вчені ступінь та звання, прізвище, ініціали) (підпис)

Рецензент _____ _____
(посада, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент_____

Київ – 2019 року

Національний технічний університет України
“Київський політехнічний інститут
імені Ігоря Сікорського”

Факультет ***Теплоенергетичний***
Кафедра ***Автоматизації теплоенергетичних процесів***
Рівень вищої освіти – другий(магістерський) за освітньо-професійною програмою

Спеціальність ***151“Автоматизація та комп’ютерно-інтегровані технології”***

ЗАТВЕРДЖУЮ

В.о.завідувача кафедри

_____ /*В.А.Волощук*/
(підпис) (ініціали, прізвище)
“ ” _____ 2019 р.

ЗАВДАННЯ
на магістерську дисертацію студенту

Яремчук Ірині Тарасівні
(прізвище, ім'я, по-батькові)

1. Тема дисертації Автоматизація процесу горіння котлоагрегату на твердому паливі

науковий керівник дисертації Ст.викладач Ю.Є.Грудзинський
(прізвище, ім'я, по-батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «4» листопада 2019 р. № 3812-с

2. Термін подання студентом дисертації «10» грудня 2019 р.

3. Об’єкт дослідження Процес горіння твердого палива в промислових водогрійних котлоагрегатах

4. Предмет дослідження (вихідні дані для магістерської дисертації за освітньо-професійною програмою) підвищення ефективності згорання палива та захист технологічного процесу від можливих втручань зовні

5. Перелік завдань, які потрібно розробити: вивчення принципу роботи об’єкту керування; побудова системи керування процесом; розробка програмного забезпечення для локального та супервізорного рівнів ПТКЗА; організація кібербезпеки підсистеми керування процесом горіння; розробка стартап-проекту.

6. Орієнтований перелік графічного (ілюстративного) матеріалу
Схема автоматизації функціональна, графіки перехідних процесів, мнемосхема об’єкта керування, схема прийнятої архітектури розшарування мережі.

7. Орієнтований перелік публікацій

1. Яремчук І.Т, Грудзинський Ю.Є. АНАЛІЗ РІВНЯ БЕЗПЕКИ І РИЗИКУ ПРИ СТВОРЕННІ СИСТЕМ «РОЗУМНИЙ БУДИНОК».Є. //Тези доповідей XVII Міжнародної науково-практичної конференції аспірантів, магістрантів і студентів «Сучасні проблеми наукового забезпечення енергетики» НТУУ «КПІ»:2019 – с.33;

2. Яремчук І.Т, Бобков В.Б. ІНТЕГРАЦІЯ МОДУЛІВ ІІОТ З СИСТЕМАМИ ВЕРХНЬОГО РІВНЯ //Тези доповідей XVII Міжнародної науково-практичної конференції аспірантів, магістрантів і студентів «Сучасні проблеми наукового забезпечення енергетики». НТУУ «КПІ»: 2019– с.34;

3. Грудзинський Ю.Є., Бунь В.П., Яремчук І.Т. Смартфон, як засіб кібератаки // Міжнародний науково-теоретичний журнал "Nauka I Studia". – Przemyśl. - 2019. - № 7(196).- с. 64-71;

8. Консультанти розділів дисертації:

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

9. Дата видачі завдання " 04 " вересня 2018 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів виконання магістерської дисертації	Строк виконання етапів магістерської дисертації	Примітка
1	*Видача завдання*	04.09.2018	
2	*Вивчення літературних джерел*	01.01.2019	
3	*Вивчення об'єкта досліджень*	01.03.2019	
4	*Підготовка тез до наукової конференції*	01.04.2019	
5	*Синтез та дослідження системи керування процесом горіння*	01.06.2019	
6	*Розробка програмного забезпечення*	01.08.2019	
7	*Вивчення питання кібербезпеки*	01.09.2019	
8	*Організація кібербезпеки*	01.11.2019	
9	*Стартап-проект*	28.11.2019	
10			
11	*Підпис керівника магістерської дисертації*	09.12.2019	
12	*Попередній захист магістерської дисертації*	10.12.2019	
13	*Захист*		

Студент _____ _____
(підпис) (прізвище та ініціали)

Науковий керівник дисертації _____ _____
(підпис) (прізвище та ініціали)

РЕФЕРАТ

Актуальність. На початковому етапі АСК ТП мало нагадували традиційні системи інформаційних технологій (ІТ), тому що АСК ТП були ізольованими системами з власними протоколами управління, що використовували спеціалізоване обладнання та програмне забезпечення. Багато компонентів АСК ТП перебували на фізично захищених ділянках, а самі компоненти не були підключені до ІТ-мереж або систем. На сьогоднішній день доступність дешевих та надійних пристроїв, які використовують протокол TCP/IP приводить до змін у корпоративних рішеннях щодо використання компонентів АСК ТП, що у свою чергу збільшує можливість вразливості та інцидентів у сфері кібербезпеки. Оскільки АСК ТП все більше використовують ІТ-рішення для можливості підключення до корпоративних бізнес-систем та використання можливостей віддаленого доступу, все більше використовують стандартні комп'ютери, операційні системи (ОС) та мережеві протоколи, то вони починають нагадувати ІТ-системи у сфері кібербезпеки. Ця інтеграція підтримується новими можливостями ІТ, але вона забезпечує значно меншу ізоляцію АСК ТП від зовнішнього світу порівняно з попередніми системами, що створює більшу потребу в безпеці цих систем.

Мета роботи і задачі дослідження. Метою даної роботи є розробка системи керування процесу горіння в котлоагрегаті із забезпеченням захисту від кібератак, а саме визначення можливих векторів атак, розшарування мережі, організація кібрбезпеки в підсистемі керування.

Головна ідея роботи полягає в розробці системи керування, яка б небула вразливою до кібератак зовні та не мала спільного трафіку з відкритими мережали, які мають доступ до інтернету. Визначення процедур та відповідальних команд за процедуру відновлення після кібератаки.

Для досягнення поставленої мети вирішувались такі завдання:

- вивчення принципу роботи об’єкту керування;
- побудова системи керування процесом;

- розробка програмного забезпечення для локального та супервізорного рівнів ПТКЗА;
- організація кібербезпеки підсистеми керування процесом горіння;
- розробка стартап-проекту.

Об’єкт дослідження. Процес горіння твердого палива в промислових Водогрійних котлоагрегатах.

Предмет дослідження. Підвищення ефективності згорання палива та захист технологічного процесу від можливих кібератак.

Методи дослідження. Поставлені задачі вирішувались з використанням загальних теоретичних відомостей про об’єкт керування в цілому і впровадження кіберзахисту підсистеми керування.

Наукова новизна отриманих результатів. Впровадження багатошарового кіберзахисту в підсистему керування котлом.

Ключові слова. Автоматизація, твердопаливний котел, кіберзахист, кібератака, багатошаровий захист.

ABSTRACT

Topicality. Initially, ICS had little resemblance to traditional information technology (IT) systems in that ICS were isolated systems running proprietary control protocols using specialized hardware and software. Many ICS components were in physically secured areas and the components were not connected to IT networks or systems. Widely available, low-cost Internet Protocol (IP) devices are now replacing proprietary solutions, which increases the possibility of cybersecurity vulnerabilities and incidents. As ICS are adopting IT solutions to promote corporate business systems connectivity and remote access capabilities, and are being designed and implemented using industry standard computers, operating systems (OS) and network protocols, they are starting to resemble IT systems. This integration supports new IT capabilities, but it provides significantly less isolation for ICS from the outside world than predecessor systems, creating a greater need to secure these systems.

Thesis objective and research tasks. The purpose of this work is to develop a control system for the combustion process in the boiler unit with protection against cyber attacks, namely the determination of possible attack vectors, network segregation, the organization of cybersecurity in the control subsystem.

The main idea of the work is to develop a management system that would not be vulnerable to cyber attacks from the outside and havent traffic with open networks that have access to the Internet. Identify procedures and responsible teams for cyber-attack recovery.

To achieve this goal, the following tasks were solved:

• study of the principle of operation of the control object;

• building a process management system;

• development of software for local and supervisory levels;

• organization of cybersecurity of the combustion process control subsystem;

• development of a startup project.

Object of research. The process of combustion of solid fuels in industrial boilers.

Subject of research. Improving fuel combustion efficiency and protecting process against possible cyber attacks.

Research methods. The tasks were solved using general theoretical information about the object of control in general and implementation of cyber defense of the control subsystem.

Scientific novelty of the obtained results. Implementation of multilayer cyber defense in the boiler control subsystem.

Keywords. Automation, solid fuel boiler, cyber defense, cyber attack, defense-in-depth.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ 10

ВСТУП 11

1. АНАЛІТИЧНИЙ ОГЛЯД ПРОБЛЕМИ 13

1.1 ОПИС ОБЄ'КТУ УПРАВЛІННЯ 13

2. РОЗХАХУНОК І МОДЕЛЮВАННЯ АТК 24

2.1 КОНТУР РЕГУЛЮВАННЯ ВМІСТУ КИСНЮ У ВИХІДНИХ ГАЗАХ 24

2.2 КОНТУР ТЕПЛОВОГО НАВАНТАЖЕННЯ 30

2.3 КОНТУР РОЗРІДЖЕННЯ В ТОПЦІ 34

ВИСНОВКИ ДО РОЗДІЛУ 2 39

3. ПРОГРАМНО-ТЕХНІЧНІ РІШЕННЯ ПТКЗА 41

3.1 ОПИС ПРОГРАМНО-ТЕХНІЧНИХ РІШЕНЬ ЛОКАЛЬНОГО РІВНЯ ПТКЗА 41

3.2 ОПИС ПРОГРАМНО-ТЕХНІЧНИХ РІШЕНЬ СУПЕРВІЗОРНОГО РІВНЯ ПТКЗА 45

3.3 ОПИС ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯЛОКАЛЬНОГО РІВНЯ ПТКЗА 47

3.4 ОПИС ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ СУПЕРВІЗОРНОГО РІВНЯ ПТКЗА 60

ВИСНОВКИ ДО РОЗДІЛУ 3 63

4. ОРГАНІЗАЦІЯ КІБЕРБЕЗПЕКИ В ПІДСИСТЕМІ КЕРУВАННЯ ПРОЦЕСОМ ГОРІННЯ КОЛОАГРЕГАТУ НА ТВЕРДОМУ ПАЛИВІ 64

4.1 ПРОЦЕДУРА ВІДНОВЛЕННЯ ПІСЛЯ КІБЕРАТАКИ 64

4.2 КОМАНДИ ЩО РЕАГУЮТЬ НА КАТАСТРОФИ 72

4.4 ІНСТРУМЕНТИ РЕАГУВАННЯ НА АТАКУ 79

4.4 КАТЕГОРИЗАЦІЯ АТАК 80

4.5 ПОМ'ЯКШЕННЯ НАСЛІДКІВ 82

4.6 ВИРІШЕННЯ ПРОБЛЕМ 83

4.7 ЗАПОБІГАННЯ ВПЛИВУ ХАКЕРІВ НА СИСТЕМИ КОТЛА 84

4.8 РОЗШАРУВАННЯ МЕРЕЖІ РОЗПОДІЛЕНОЇ СИСТЕМИ КЕРУВАННЯ КОТЛОАГРЕГАТОМ 86

ВИСНОВКИ ДО РОЗДІЛУ 4 96

5 РОЗРОБКА СТАРТАП-ПРОЕКТУ 97
5.1 ОПИС ІДЕЇ ПРОЕКТУ 97
5.2 ТЕХНОЛОГІЧНИЙ АУДИТ ІДЕЇ ПРОЕКТУ 98
5.3 АНАЛІЗ РИНКОВИХ МОЖЛИВОСТЕЙ ЗАПУСКУ СТАРТАП-ПРОЕКТУ 99
5.4 РОЗРОБКА РИНКОВОЇ СТРАТЕГІЇ ПРОЕКТУ 105
5.5 РОЗРОБКА МАРКЕТИНГОВОЇ ПРОГРАМИ СТАРТАП- ПРОЕКТУ 107
ВИНОВКИ ДО РОЗДІЛУ 5 109
ВИСНОВКИ 110
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 112

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АСУ ТП – автоматична система управління технологічним процесом;

ТОУ – технологічний об’єкт управління;

РО – регулюючий орган;

ВМ – виконавчий механізм;

ФСА – функціональна схема автоматизації;

ПТКЗА – програмно-технічний комплекс засобів автоматизації;

ПК – персональний комп’ютер;

ПЛК – програмно-логічний контролер;

ПЗ – програмне забезпечення;

РСТ – робоча станція обробки текстової інформації;

HMI – Human Machine Interface;

SCADA – Supervisory Control and Data Acquisition;

TCP/IP – Transmission Control Protocol / Internet Protocol;

ПІ-регулятор – пропорційно-інтегральний регулятор;

ПІД-регулятор – пропорційно-інтегрально-диференціальний регулятор;

РАФХ – розширена амплітудно-фазова характеристика;

АП-2 – аперіодична ланка другого порядку;

РСК – розподілена система керування;

MGMT – Recovery Management Team;

FAC – Recovery Facilities Team;

TECH – Recovery Tech Support Team;

ВСТУП

В наш час спостерігаються дві тенденції в системах керування – це перехід засобів управління на стандарт Ethernet та винекнення специфічного шкідливого програмного забезпечення орієнтованого на промислові системи керування. З одного боку використання ІТ-рішень в АСК ТП збільшує її можливості, виводячи автоматизацію на новий рівень, але з іншого вона набула всі вразливості притаманні ІТ.

З розвитком інформаційних технологій підприємства все частіше впроваджують ERP системи, які виконують функцію планування та управління виробництвом представляючи корпоративну мережу, яка часто потребує дані від промислової мережі і це може становити серйозну загрозу. Характер мережевого трафіку в цих двох мережах різний: доступ до Інтернету, електронна пошта та віддалений доступ, як правило, допускається в корпоративній мережі, але не повинен бути дозволений в мережі АСК ТП. Суворі процедури контролю заміни для мережевого обладнання, конфігурації та зміни програмного забезпечення можуть не мати місце в корпоративній мережі. Якщо мережевий трафік АСК ТП здійснюється в корпоративній мережі, він може бути перехоплений або піддаватися атаці.

Можливість доступу зовнішнього світу до АСКТП підвищує ймовірність кібератаки і втручання в технологічний процес підприємства, що може спричинити серйозні матеріальні, людські втрати та втрату довіри й репутації компанії.

На даний час в Україні питання кібербезпеки систем керування не часто порушують, тому ми вважаючи на це та на політичну ситуацію в країні, ми є привабливою ціллю для кіберзлочинців.

Об’єктом дослідження є водогрійний котел на твердому паливі який є потенційно небезпечним об’єктом і потребує підвищеного рівня безпеки. А наявність дистанційного управління та зв’язку з корпоративною мережею компанії, визначає нагальність створення та організації безпечної системи керування котлом.

Так як у випадку виходу із ладу автоматики кола, можуть виникнути небезпечні ситуації такі як перегріву труб, загорання в димоході до вибуху котла, що в результаті несе за собою пошкодження обладнання, простій виробництва і загрозу для життя і здоров’я працюючого персоналу.

1. АНАЛІТИЧНИЙ ОГЛЯД ПРОБЛЕМИ

1.1 ОПИС ОБЄ'КТУ УПРАВЛІННЯ

Твердопаливний водогрійний котел КВм-1,75 знаходиться на підприємстві з виготовлення паркету ТОЗОВ «Таркетт-Вінісін» в місті Калуш. Котел забезпечує опалення, гаряче водопостачання та три сушильні камери для сушки деревини. Паливом для котла служать відходи від виробництва(дерев'яна стружка).

Основні характеристики котлоагрегата наведені в таблиці 1.

Таблиця 1.1 Основні характеристики котлоагрегата

Характеристика		Опис
Число ліній нагріву		1
Потужність котла на деревині 15% вологості Потужність котла на деревині 30% вологості Потужність котла на деревині 45% вологості Потужність котла на деревині 55% вологості		2 700 кВт 2 500 кВт 2 300 кВт 2 100 кВт
Охолоджуюча рідина		Вода
Максимальна температура охолоджуючої рідини		109°C
Протік		$86\,^{м^3}/_{год}$
Тиск		6 бар
Приєднувальна потужність		47 кВт
Гарантії викидів в атмосферу	Пил	150 mg/Nm3 сухої 11% d`O2
	CO	250 mg/Nm3 сухої 11% d`O2
	NO2	500 mg/Nm3 сухої 11% d`O2
	COV	50 mg/Nm3 сухої 11% d`O2

Продовження Таблиці 1.1

Характеристики палива	Потужність внутрішньої тепловіддачі(PCI)	Від 4210 кВч/t для деревини 15% вологості до 1930 кВч/t для деревини 55% вологості
	Вологість	Від 15% до 55%
	Густина	Від 200 для деревини 15% вологості до 400 кг/м^3 для деревини 55% вологості
	Кількість пилу	3% (<1mm)
Складування палива		Пристрій «живе дно»
Транспортування палива до котла		Ланцюговий транспортер
Подача палива в котел		Пристрій паливоподачі шнекового типу (УТП)
Тип топки		Механічна колосникова решітка
Розподіл спалюваного повітря		Первинне, вторинне повітря
Тип теплообмінника		Двоходовий трубний теплообмінник
Обладнання для обробки диму		Мультициклон
Видалення золи з під топки		Вологе золовидалення під колосниками до ковша-прийомника золи і шнекове під мультициклоном
Час ходу «живого дна»		1/10 с

До складу котла входять такі основні вузли і блоки :

- Котел(рама з рухливими колосниками, топка з теплообмінником, двері нижні і технологічні, мультициклон);
- Облаштування паливоподачі(плунжер або шнек);
- Комплект вентиляторів;
- Димосос;

- Система золовидалення;

- Запобіжні клапана і гідророзводка;

- Система автоматики з датчиками управління і контролю. Контроль процесу горіння з кисневого зонду.

- Система пневмоочистки теплообмінника котла.

Паливо подається шнеком(1) в канал подання(2), потім подається в топку(3), яка в основі має рухливу чавунну колосникову решітку(4). Кожен другий ряд встановлений на

рухливій балці(5), яка рухається в «перед» «назад». Частина рядів - рухлива, частина - ні, що забезпечує переміщення палива по колосникових гратах. Рух рами відбувається за рахунок гідравлічного циліндра, який наводиться в рух за допомогою гідростанції, яка входить в комплект постачання. Хід циліндра контролюється датчиками.

У топці паливо зазнає різним трансформаціям.

- При попаданні в топку, волога, що міститься в паливі, випаровується завдяки високій температурі в топці(виділення білого диму).

- Коли уся волога випаровується, усередині топки утворюється леткий паливний газ, вивільнений піролізом. Деревина - це паливо, що містить приблизно 70% летких речовин.

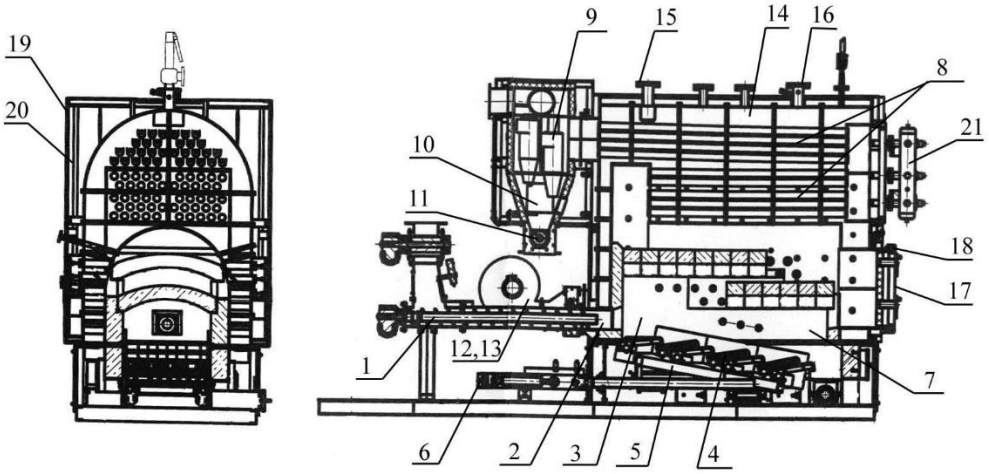
- Тверда фракція, яка залишилася після звільнення газу піролізом, горить по напряму вниз топки. У кінці колосникових грат, горіння закінчується і залишається тільки зола.

- Летка фракція палива, вивільнена піролізом, горітиме в газовій фазі. Це горіння починається в топці, над колосниковими гратами, потім триває в першому проході циркуляції димових газів(чи камері згорання). Цей паливний простір досить просторий для тривалого знаходження часток, що летять з топки і виснажуються в полум'ї горіння.

Для організації такого горіння, нагнітання підтримувального горіння повітря організовано таким чином:

- Первинне повітря нагнітається під колосникові грати, в різні відділення

трансформації палива, що відповідають різним фазам, що пов'язані з колосниковими гратами(сушка, піроліз, горіння вуглистих залишків). Установки, передбачені для спалювання дуже вологого палива, можуть бути оснащені системою попередньої сушки палива : гарячі гази спрямовуються в нижню частину топки і змішуються з повітрям, що нагнітається під колосники при вході в топку. На деяких установках, навпаки, холодні гази подаються на рівень обробки димових газів для змішування з повітрям, йдеться про «розбавлене первинне повітря»: метою є створити достатній для охолодження колосників потік, не збільшуючи загальну кількість кисню під колосниками для здійснення поверхового горіння.



1 – шнек; 2 - канал подання палива; 3 - топка; 4 - чавунні колосники; 5 - балка; 6 – гідравлічний циліндр; 7 - камера спалювання; 8 - трубний пучок; 9 - мультициклон; 10 - бункер; 11 - шнек транспортування золи; 12 - вентилятор вторинного повітря; 13 - вентилятор первинного повітря; 14 - теплообмінник; 15 - подаючий водяний патрубок; 16 - зворотний водяний патрубок; 17 - нижні дверці; 18 - оглядове вікно; 19 - кожух; 20 - теплоізоляція; 21 - система пневмоочистки теплообмінника котла; 22 - запобіжний клапан.

Рис. 1.1 Котел водогрійний опалювальний КВм-1,75

-Вторинне повітря вдувається через отвори нагорі котла, на рівні проходу до першого ряду трубного теплообмінника : це повітря забезпечує горіння газів піролізу. Отвори оснащені заглушками, регульованими в ручному режимі зовні котла, можна також регулювати їх число і розміщення.

Кількість вентиляторів визначена виходячи з максимального необхідного протоки, тобто максимальної потужності. Для потужності нижче номінальною протока повітря зменшується за допомогою регістрів і варіаторів, пов'язаних з вентиляторами(згідно установки). Протока вторинного повітря також регулюється залежно від бажаної кількості кисню на виході з котла.

Реалізація горіння у декілька етапів - це техніка «ступінчастого горіння», яка використовується для досягнення більшої ефективності горіння при найменшій кількості забруднюючих речовин. Горіння відбувається не лише на рівні колосників, температура там менш висока, що дозволяє зменшити виробництво оксиду азоту термічного походження. Продукти з першої зони горіння закінчують горіти на рівні нагнітання вторинного повітря, де розвивається живе полум'я, і там же відбувається трансформація З в CO2.

Більше того, щоб значно зменшити утворення оксиду азоту(Nox), деякі котли оснащені облаштуванням рециркуляції димових газів(в основному це котли для спалювання дуже сухого палива, або палива, що містить елементи, сприяючі утворенню Nox, наприклад, паливо, багате на азот) : димові гази після стадії обробки, нагнітаються назад в котел поверх колосників по усій їх довжині. Це нагнітання газів, бідних на кисень, дозволяє зменшити утворення оксиду азоту. Оскільки подання палива здійснюється шнеком, паливо збирається в каналі подання, потім потрапляє в топку, що включає рухливі колосники. Ці колосники влаштовані на чавунній балці з високим вмістом хрому і розташовані рядами. Кожен другий ряд розташований на рамі, що рухається, яка забезпечує рух вперед-назад : ці ряди таким чином - що рухаються, тоді як інші - нерухомі. Ця система допомагає паливу поширюватися по колосниках:

- коли рама, що рухається, йде вперед, балки, що рухаються, ковзають по нерухомих і штовхають паливо вперед

- коли рама, що рухається, йде назад, балки, що рухаються, ковзають під нерухомими: паливо, що знаходиться на балках, що рухаються, потрапляє на нерухомі.

Раму, що рухається, приводить в рух гідравлічний циліндр. Хід циліндра

контролюється двома датчиками наближення, які розташовані у кінці руху для визначення проходження сережки . Для котлів, площа колосників яких велика, колосники розділяються на секції, які наводяться в рух окремо один від одного.

Бічні стінки і стеля топки покриті теплоізоляційним бетоном. Цей матеріал дозволяє підтримувати достатню для ефективного горіння в топці температуру.

Розрідження в топці створюється димососом. При автоматичному управлінні димосос служить для видалення димів і підтримки постійного розрідження в топці. Розрідження вимірюється і регулюється за заданою величиною(8 ммСЕ) швидкістю димососа через частотний перетворювач.

Димосос може працювати в ручному режимі: це використовується для прискорення охолодження топки для погашення вогню і очищення від золи при щорічному ручному очищенні.

Залежно від установки, протока повітря змінюється від швидкості вентиляторів через варіатори і/або завдяки засувкам.

Для первинного повітря, швидкість вентилятора/ів і кількість відкритих заслінок дають мінімальну або максимальну потужність, в автоматичному режимі ці налаштування виконуються від середньої потужності.

Для вторинного повітря, швидкість вентилятора в автоматичному режимі настроюється від середньої потужності. Кількість відкритих заслінок змінюється залежно від заданих параметрів диоксигена, який вимірюється постійно на виході димососа. Мінімальне і максимальне відкриття заслінок задаються для різних потужностей.

Для правильного регулювання, треба спиратися на наступні принципи:

- Необхідно підтримувати мінімальну протоку первинного повітря, оскільки він захищає колосники охолодженням.

- Розподіл повітря повинен дозволити здійснювати ступінчасте горіння: якщо протока первинного повітря занадто велика, горіння відбувається на рівні колосників і кількість відкритих заслінок вторинного і третинного повітря занадто маленька для другої фази ефективного горіння. Занадто велика кількість первинного повітря також сприяє літанню часток в топці.

- Ступінь відкриття заслінки вторинного повітря повинна дозволяти регулювати кількість кисню.

- Регулювання повинне робитися з частим візуальним контролем топки завдяки віконцю на дверях топки. Це дозволить бачити горіння в топці і перевірити ступінчастість горіння : не повинне з'являтися біле полум'я(занадто велика кількість первинного повітря), полум'я повинне утворюватися вверху топки і зона горіння має бути добре видна.

Для здійснення регулювання, рекомендується використати вимірювальні прилади, що дозволяють перевірити кількість моноксиду карбону, діоксиду карбону і кисню в димових газах. Для здійснення правильних вимірів необхідно дочекатися рівномірної роботи котла.

При зупинці котла(або при термостатичній або через помилку) заслінки первинного повітря закриваються, а заслінки вторинного - відкриваються до заданої величини для провітрювання зони горіння.

Після теплообмінника димові гази поступають в мультициклон: це облаштування обробки димових газів прибирає найбільші частки і дозволяє на виході зменшити число часток до 150 мг/м3.

Цей мультициклон складається з деякої кількості циклонів : димові гази поступають по дотичній в циклони, де клубочаться. Таким чином частки відділяються силою центрифуги і падають під циклони, а димові гази спрямовуються вгору і віддаляються. Частки збираються під мультициклоном в ємність і віддаляються через герметичний шлюз. Герметичність - ця необхідна умова нормальної роботи циклонів. Зола потім транспортується до видалення шнеком.

Котел виготовлений з товстолистової сталі, топка футерована жаростійким бетоном, утепленою базальтовим утеплювачем. Усі елементи котельної установки змонтовані на загальній рамі.

Система автоматизованої паливоподачі призначена для автоматизованого прийому сипкого палива, транспортування і розподілу його до живлячих паливних бункерів котлів, розташованих послідовно на одній лінії. Допустима

фракція палива не повинна перевищувати розмірів 8х8х40 мм з сумарною вологістю не більше 10%.

Комплект постачання САТ 019 «Силос»:

- місткість каркасного типу для безтарного зберігання палива 100 м3(1);
- транспортер шнековий(2);
- перетрушувач-дозатор(3);
- система автоматизованого управління і контролю рівня палива(4).

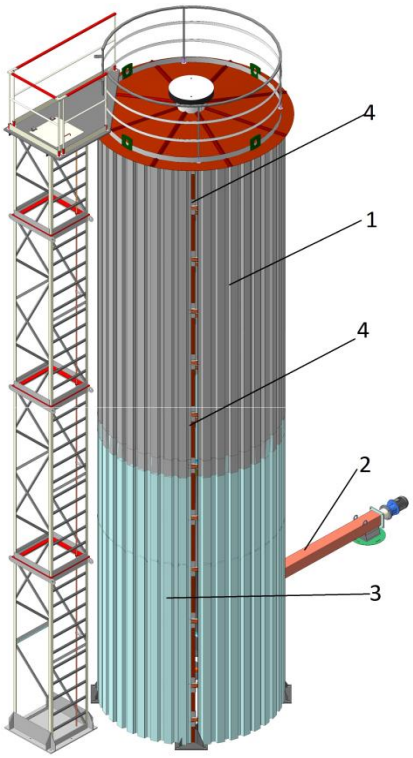


Рис. 1.2 Система САТ 019 «Силос»

Система САТ 019 є готовим модульним виробом, усі елементи системи змонтовані на загальному каркасі 100% зібраних на заводі, що значно полегшує монтаж цього устаткування і мінімізує витрати пов'язані з роботами по проектуванню і виготовленню фундаментів.

Завантаження силосу робиться механізовано. Для цього застосовують послідовну систему приймального бункера і ковшовий транспортер(норія), або ж використовують систему пневмозагрузки.

Паливо з місткості подається через перетрушувач-дозатор шнековим транспортером(поз. 2) у витратний бункер котла. Система автоматизованого управління забезпечує контроль рівня палива у витратних бункерах котлів,

зупинку роботи системи при виникненні аварії, звукове і світлове попередження про роботу, захист від перевантаження транспортерів. У котел паливо подається за допомогою облаштування подання палива шнекового типу. Усередині топки утворюється леткий паливний газ, вивільнений піролізом. Тверда фракція горить по напряму вниз топки. У кінці колосникових грат, горіння закінчується і залишається тільки зола. Летка фракція палива, горить в газовій фазі. Це горіння починається в топці, над колосниковими гратами, потім триває в першому ході(чи камері згорання). Цей паливний простір досить просторий для тривалого знаходження часток, що летять з топки і виснажуються в полум'ї горіння. Щоб організувати таке горіння, нагнітання підтримувального горіння повітря організовано таким чином:

- Первинне повітря нагнітається під колосникові грати, в різні відділення трансформації палива(піроліз, горіння вуглистих залишків), що відповідають різним фазам.
- Вторинне повітря вдувається через отвір в котлі, на рівні проходу до першого ряду трубного теплообмінника : це повітря забезпечує горіння газів піролізу. Отвір оснащений заглушками.

Для потужності нижче номінальною протока повітря зменшується за допомогою автоматичних заслінок і частотних регуляторів оборотів вентиляторів. Протока вторинного повітря також регулюється залежно від бажаної кількості кисню на виході з котла.

Реалізація горіння у декілька етапів - техніка «ступінчастого горіння», використовується для досягнення більшої ефективності горіння при найменшій емісії забруднюючих речовин. Горіння відбувається не лише на рівні колосників, температура там менш висока, що дозволяє зменшити емісію оксиду азоту термічного походження. Продукти з першої зони горіння закінчують горіти на рівні нагнітання вторинного повітря, де розвивається живе полум'я, і там же відбувається трансформація З в СО2.

Спеціальна конструкція колосників передбачає роботу грат «без просипів», що забезпечує мінімальні втрати від «механічного недопалу» і

спрощує обслуговування основи котла. Кожен другий ряд колосників розташований на рамі, що рухається, яка забезпечує їх циклічний рух. Ця система допомагає паливу рівномірно розподілятися по колосниках:

- коли рухлива рама йде вперед, рухливі колосники ковзають по нерухомих і штовхають паливо вперед;
- коли рама йде назад, паливо, що знаходиться на рухливих колосниках потрапляє на нерухомі.

Раму приводить в рух гідравлічний циліндр. Хід циліндра контролюється двома датчиками, які розташовані в кінцевих точках руху.

Для зменшення впливу хлору на корозію поверхонь нагріву топки котла, максимальний зміст якого може досягати 0,97 % елементарного складу сухої соломи - топка захищена теплоізоляційним бетоном з високим вмістом Al2O3. Для зменшення викидів оксиду азоту(масимальное вміст азоту може досягати 0,6 % елементарного складу сухої соломи) у тому числі використовується технологія повернення частини продуктів згорання в топку котла. Оскільки розм'якшення золи соломи починається при дуже низьких температурах(біля 7000С) - використовується декілька технологічних рішень:

- технологія спалювання пелети передбачає інтенсивне «охолодження» топки за рахунок використання повітря охолоджуваних зведень топки і повітря охолоджуваних колосникових грат;
- активне використання технології рециркуляції димових газів топки для запобігання шлакуванню колосникових грат.

Відпрацьовані димові гази з топки проходячи через камеру допалу і двоходовий трубний пучок, віддають тепло теплоносію. Далі слідують в мультициклон, коефіцієнт корисної дії, якої, складає не менше 97%. Мультициклон передбачений для очищення димових газів, що виходять з опалювального котла, від твердих часток. Застосування литих корпусів циклонів із спеціального матеріалу, дозволяє значно збільшити термін експлуатації цього вузла навіть в умовах максимальної абразивності часток, що очищаються.

Димові гази потрапляють в мультициклон по спіралеподібній поверхні і під дією відцентрових сил тверді частки осідають в нижній бункер, звідки за допомогою шнекового транспорту переміщаються в загальну систему золовидалення, а гази виходять через верхню частину циклону.

Розрідження в топці створюється димососом. Димосос призначений для видалення димових газів з котла через мультициклон в димар.

Система пневматичного очищення димогарних труб завершує комплекс систем що зводять до мінімуму участь людини в роботі котла і дає можливість повною мірою використати усі можливості устаткування. Ця система через мультициклон включена в загальну систему золовидалення котла. Зола віддаляється автоматично в спеціальні ємності для золи. Усі елементи котельної установки змонтовані на загальній рамі, що значно полегшує монтаж цього устаткування і мінімізує витрати пов'язані з роботами по проектуванню і виготовленню фундаментів.

2. РОЗХАХУНОК І МОДЕЛЮВАННЯ АТК

2.1 КОНТУР РЕГУЛЮВАННЯ ВМІСТУ КИСНЮ У ВИХІДНИХ ГАЗАХ

2.1.1 ОТРИМАННЯ ПЕРЕХІДНОЇ ХАРАКТЕРИСТИКИ

Перехідна характеристика – це реакція об’єкту на одиничне ступінчате збурення. Використаємо передаточну функцію об’єкта керування вмісту кисню в газах на виході з котла, який регулюється шляхом зміни ступеня відкриття заслінки вторинного повітря, з технологічного регламенту[9]:

$$W_{об1} = \frac{0{,}1}{27s+1} e^{-52s}$$

$\tau_{об1} = 52c$; $T_{об1} = 27c$; $K_{об1} = 0{,}1 \%/\%ходуВМ$

Цей об’єкт належить до об’єктів з самовирівнюванням. Такий об’єкт апроксимується послідовним з’єднанням ланки транспортного запізнення та аперіодичної ланки першого порядку.[4]

2.1.2 РОЗРАХУНОК РЕГУЛЯТОРА

Для контуру регулювання вмісту кисню у вихідних газах оберемо ПІ-закон регулювання, розрахунок параметрів регулятора виконаємо трьома методами:

1. Метод РАФХ(Розширеної амплітудно-фазової характеристики)
2. Два інженерні методи

Метод РАФХ забезпечує точність оптимізації налаштувань одноконтурних систем з типовими законами регулювання: пропорційним, інтегральним й пропорційно-інтегральним. Суть метода заключається у наступному.

Передаточна функція замкнутої одноконтурної системи дорівнює:

$$W_{зс}(p) = \frac{W_{об}(p)}{1 + W_p(p) W_{об}(p)} \quad (2.1)$$

де $W_{об}(p)$ *и* $W_p(p)$ - передаточні функції відповідного об’єкта керування та регулятора. Звідси характеристичне рівняння замкнутої системи має вигляд:

$$1 + W_p(p) W_{экв}(p) = 0 \quad (2.2)$$

Виразимо розширені АФХ об’єкта керування та регулятора через їх дійсні і уявні частини:

$$W_{экв}(m,\omega) = P_{экв}(m,\omega) + iQ_{экв}(m,\omega)$$
$$W_p(m,\omega) = P_p(m,\omega) + iQ_p(m,\omega) \qquad (2.3)$$

Підставляючи в (2.2) значення (2.3), отримаємо рівняння границі заданого ступеню коливальності $m = const$

$$1 + [P_{экв}(m,\omega) + iQ_{экв}(m,\omega)][P_p(m,\omega) + iQ_p(m,\omega)] = 0 \qquad (2.4)$$

Далі розглянемо метод стосовно до розрахунку ПІ-регулятора, оскільки в часткових випадках такий підхід дає можливість визначати настройку П- та І-регуляторов.

Передаточна функція ПІ-регулятора

$$W_p(p) = k_n(1 + \frac{1}{T_n p}) \qquad (2.5)$$

де k_n - коуфіціент передачі, T_n - постійна інтегрування. Другий параметр налаштування приміняється також у формі коефіціента передачі по інтегралу:

$$K_h = \frac{K_n}{T_h} \quad (2.6)$$

Розширена АФХ регулятора отримується з (2.5), з урахуванням відношення (2.6) підстановкою $p = \omega(i - m)$:

$$P_p(m,\omega) = k_n - \frac{k_n m}{\omega(m^2 + 1)}$$
$$Q_p(m,\omega) = -\frac{k_n}{\omega(m^2 + 1)} \qquad (2.7)$$

З рівняння (2.4) підстановкою значень розширеної АФХ регулятора з виразу 2.7) отримуємо розрахункові формули для визначення пар налаштування регулятора в координатах k_n та $k_h = {k_n}/{T_n}$ через складові розширеної АФХ об’єкта керування:

$$k_n = -\frac{mQ_{об}(m,\omega) + P_{об}(m,\omega)}{A^2_{об}(m,\omega)}$$
$$k_h = -\omega(m^2+1)\frac{Q_{об}(m,\omega)}{A^2_{об}(m,\omega)} \quad (2.8)$$
$$A_{об}(m,w) = \sqrt{P^2_{об}(m,w) + Q^2_{об}(m,w)}$$

В результаті отримуємо набір параметрів, що задовольняють задані умови.[4]

Обираємо для розрахунку налаштувань регулятора ступень коливальності $m = 0.45$, за якого показник затухання $\psi = 0.94$.

Скориставшись формулами для ПІ-регулятора(2.8), будуємо залежність в координатах Ki і Kp:

```
m=0.45;
w=0:0.00001:0.039;
p=-m*w+i*w;
W=(0.1*exp(-52.*p))./(27.*p+1);
Re=real(W);
Im=imag(W);
Kp=-(m.*Im+Re)./(Im.^2+Re.^2);
Ki=-w.*(m.^2+1).*Im./(Im.^2+Re.^2);
plot(Kp,Ki,'-b');
grid on;
ylabel('Ki');
xlabel('Kp');
```

Отримана крива зображена на рис 2.1. На даній криві вибираємо точку, що відповідає мінімальному інтегральному критерію якості, яка лежить справа і дорівнює $0{,}95Ki^{\max} = 0{,}1377$

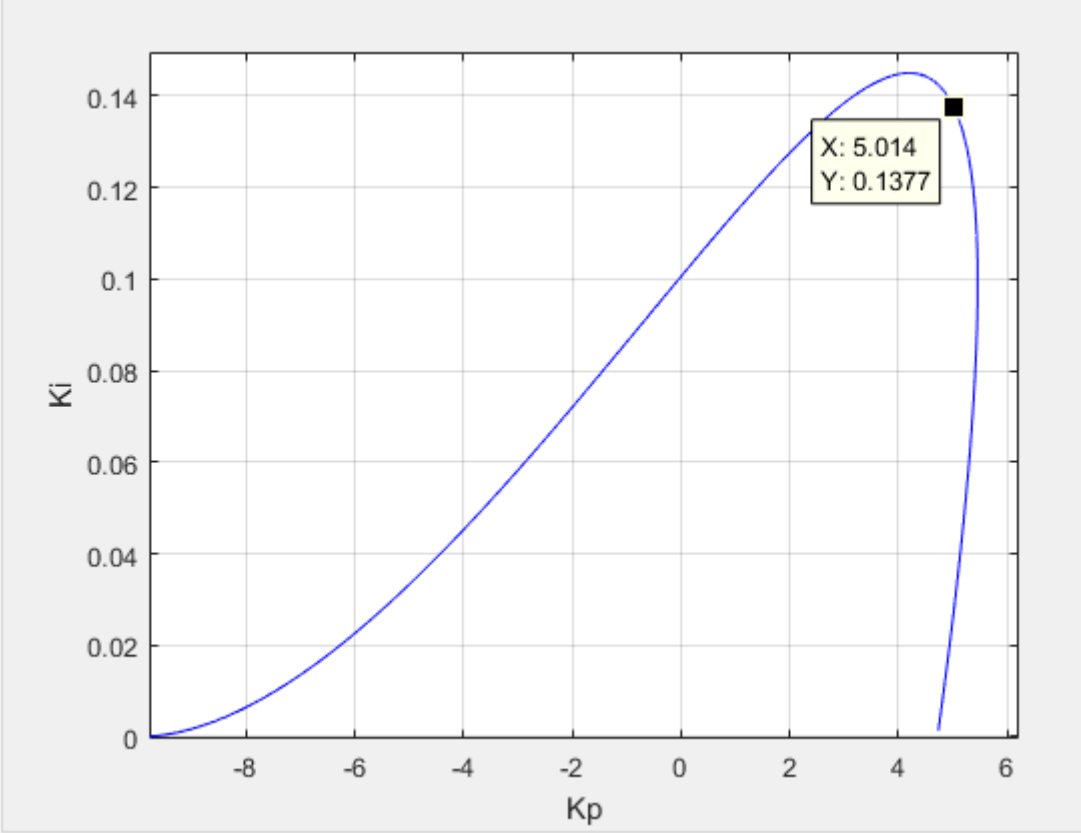


Рис.2.1 Крива налаштувань K_p , K_i контуру регулювання вмісту кисню у вихідних газах

Таким чином параметри ПІ регулятора наступні $K_p = 5.014$, $K_\text{i} = 0.1377$, $\text{T}_\text{i} = 36.41$, а передаточна функція має вигляд:

Обрано інженерні методики, які так як метод РАФХ забезпечують мінімальний інтегральний критерій якості, а саме:

1) Minimum ISE - Haalman(1965): $K_p = \frac{0.67T_o}{K_o\tau_o}$, $T_i = T_o$ [7]

2) Minimum ISE - Zhuang and Atherton (1993): $K_p = \frac{1.346}{K_o}(\frac{T_o}{\tau_o})^{0.675}$, $T_i = \frac{T_o}{0.552}(\frac{\tau_o}{T_o})^{0.438}$ [7]

Розрахуємо налаштування регулятора згідно наведених методик і отримаємо:

1) $K_p = \frac{0.67 * 27}{0.1 * 52} = 3.48$, $T_i = 27$

2) $K_p = \frac{1.346}{0{,}1}(\frac{27}{52})^{0.675} = 8.65$, $T_i = \frac{27}{0.552}(\frac{52}{27})^{0.438} = 65.18$

Побудуємо перехідні процеси для замкненої САР для вибору отимальних налаштувань регулятора за допомогою пакету Matlab та розрахуємо прямі показники якості перехідного процесу по каналам «завдання – вихід» та «збурення – вихід»(рис.2.2).

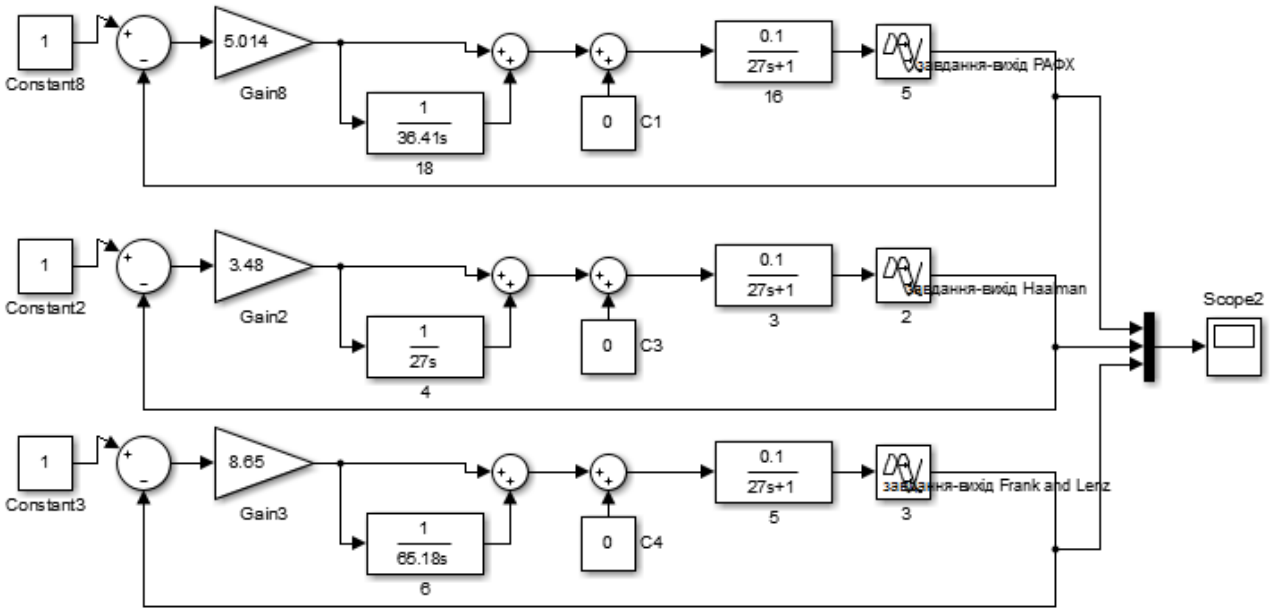


Рис. 2.2 Змодельована схема в середовищі Matlab

Результати моделювання наведені на рис.2.3 та 2.4.

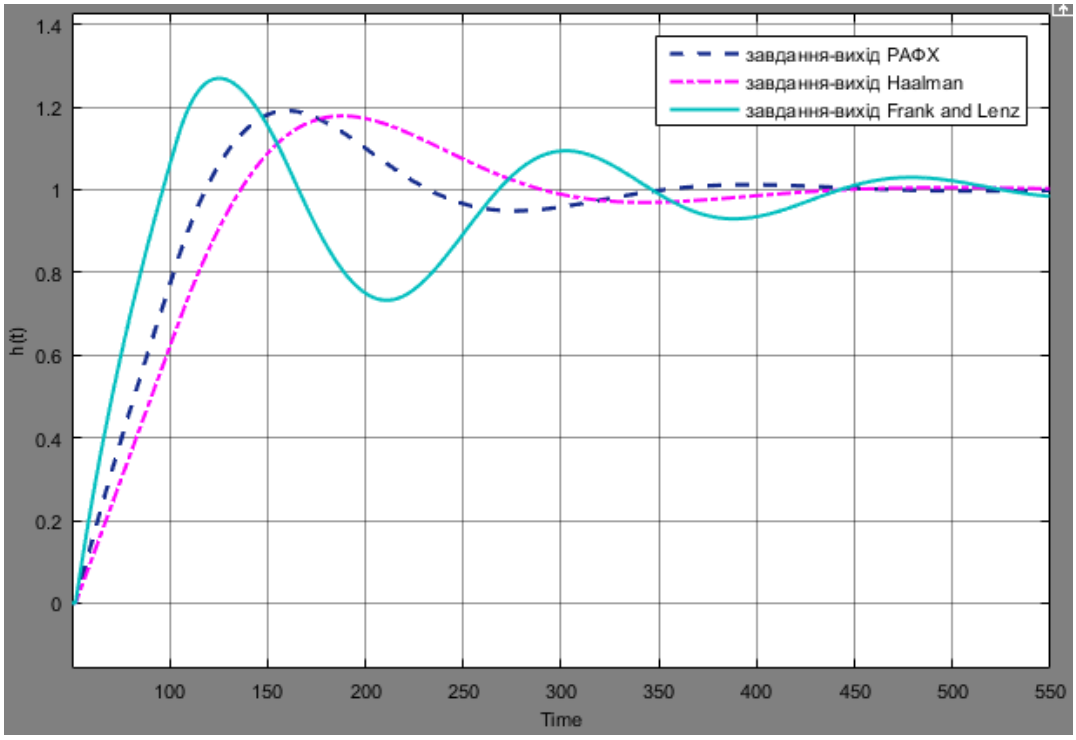


Рис. 2.3 Перехідні процеси по каналу «завдання-вихід»

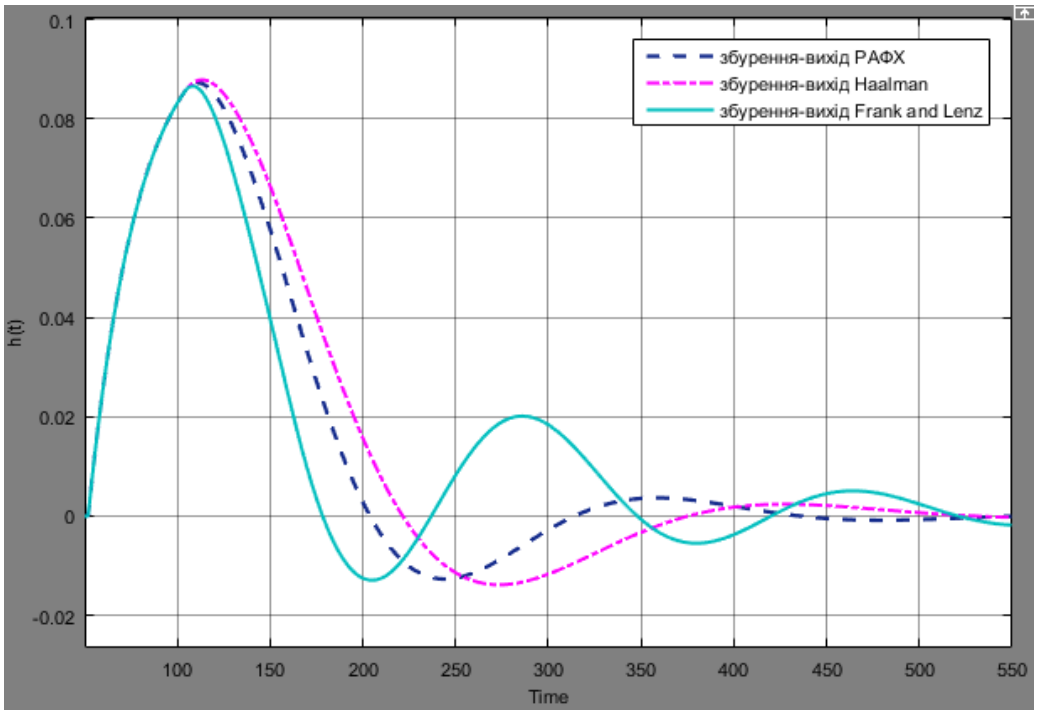


Рис.2.4 Перехідні процеси по каналу «збурення-вихід»

Розрахуємо прямі показники по каналу завдання-вихід та збурення-вихід з налаштуваннями регулятора отриманими інженерними методиками та методом РАФХ. Результати розрахунків наведені в таблиці 2.1

Таблиця 2.1 Показники якості для контуру вмісту кисню у вихідних газах

Показник якості	«завдання-вихід»			«збурення-вихід»		
	РАФХ	Haalman	Zhuang and Atherton	РАФХ	Haalman	Zhuang and Atherton
Статична помилка $\Delta_{ст}$	0	0	0	0	0	0
Динамічна помилка $\Delta_{дин}$	0,191	0,1785	0,27	0,0872	0,0878	0,0865
Степінь затухання ψ	0,937	0,97	0,65	0,958	0,973	0,768
Час регулювання $t_{рег}$	282	261	413	292	343	482
Перерегулювання σ, %	19,1	17,85	27	6.87	6.34	6.69

Порівнюючи прямі показники якості перехідних процесів з використанням різних регуляторів і враховуючи те, що для нашого об’єкта важливим критерієм є невеликий час регулювання та перерегулювання можемо зробити висновок, що ПІ-регулятор розрахований методом Haalman є оптимальнішим вибором.

2.2 КОНТУР ТЕПЛОВОГО НАВАНТАЖЕННЯ

2.2.1 ОТРИМАННЯ ПЕРЕХІДНОЇ ХАРАКТЕРИСТИКИ

Використаємо передаточну функцію об’єкта керування теплового навантаження в твердопаливному котлі з технологічного регламенту [9]:

$$W_{об1} = \frac{1}{120s+1} e^{-60s}$$

$\tau_{об1} = 60c$; $T_{об1} = 120c$; $K_{об1} = 1 {}^{C^0}\!\!\diagup\!\!{}_{\%ходуВМ}$

Цей об’єкт належить до об’єктів з самовирівнюванням. Такий об’єкт апроксимується послідовним з’єднанням ланки транспортного запізнення та аперіодичної ланки першого порядку.[4]

2.1.2 РОЗРАХУНОК РЕГУЛЯТОРА

Для контуру регулювання вмісту кисню у вихідних газах оберемо ПІ-закон регулювання, розрахунок параметрів регулятора виконаємо трьома методами:

1. Метод РАФХ(Розширеної амплітудно-фазової характеристики)
2. Два інженерні методи

Метод РАФХ забеспечує точність оптимізації налаштувань одноконтурних систем з типовими законами регулювання: пропорційним, інтегральним й пропорційно-інтегральним.

Обираємо для розрахунку налаштувань регулятора ступень коливальності $m = 1.47$, за якого показник затухання $\psi = 0.94$.

Скориставшись формулами для ПІ-регулятора(2.8), будуємо залежність в координатах Ki і Kp:

m=0.45;

w=0:0.0000001:0.0247;

```
p=-m*w+i*w;
W=(1*exp(-60.*p))./(120.*p+1);
Re=real(W);
Im=imag(W);
Kp=-(m.*Im+Re)./(Im.^2+Re.^2);
Ki=-w.*(m.^2+1).*Im./(Im.^2+Re.^2);
plot(Kp,Ki,'-b');
grid on;
ylabel('Ki');
xlabel('Kp');
```

Отримана крива зображена на рис 2.5. На даній криві вибираємо точку, що відповідає мінімальному інтегральному критерію якості, яка лежить справа і дорівнює $0{,}95Ki^{max} = 0{,}01449$

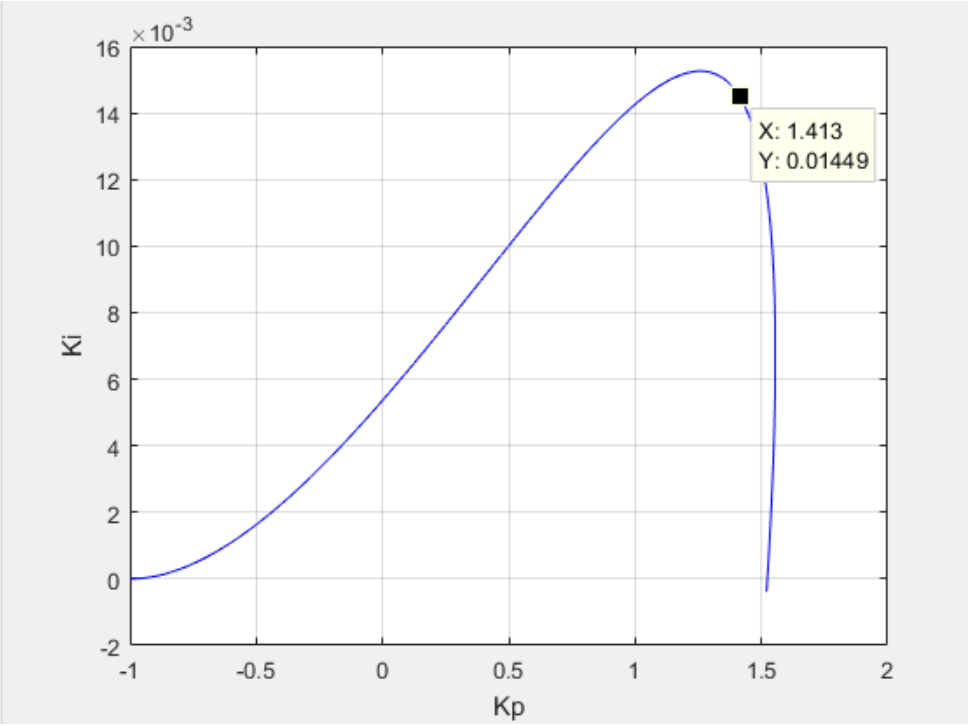


Рис.2.6 Крива налаштувань K_p , K_i контуру регулювання вмісту кисню у вихідних газах

Таким чином параметри ПІ регулятора наступні $K_p = 1.413$, $K_\text{i} = 0.01449$, $\text{T}_\text{i} = 97.52$, а передаточна функція має вигляд:

Обрано інженерні методики, які так як метод РАФХ забезпечують мінімальний інтегральний критерій якості, а саме:

1. Minimum ISE - Haalman(1965): $K_p = \frac{0.67T_o}{K_o\tau_o}$, $T_i = T_o$ [7]

2. Minimum ISE - Frank and Lenz (1969): $K_p = \frac{1}{K_o}(0.595 + 0.925\frac{T_o}{\tau_o})$,

$T_i = \frac{\tau_o}{0.925}(0.595 + 0.925\frac{T_o}{\tau_o})$ [7]

Розрахуємо налаштування регулятора згідно наведених методик і отримаємо:

1. $K_p = \frac{0.67 * 120}{1 * 60} = 1.34$, $T_i = 120$

2. $K_p = \frac{1}{1}(0.595 + 0.925\frac{120}{60}) = 2.445$, $T_i = \frac{60}{0.925}(0.595 + 0.925\frac{120}{60}) = 158{,}595$

Побудуємо перехідні процеси для замкненої САР для вибору отимальних налаштувань регулятора за допомогою пакету Matlab та розрахуємо прямі показники якості перехідного процесу по каналам «завдання – вихід» та «збурення – вихід»(рис.2.7).

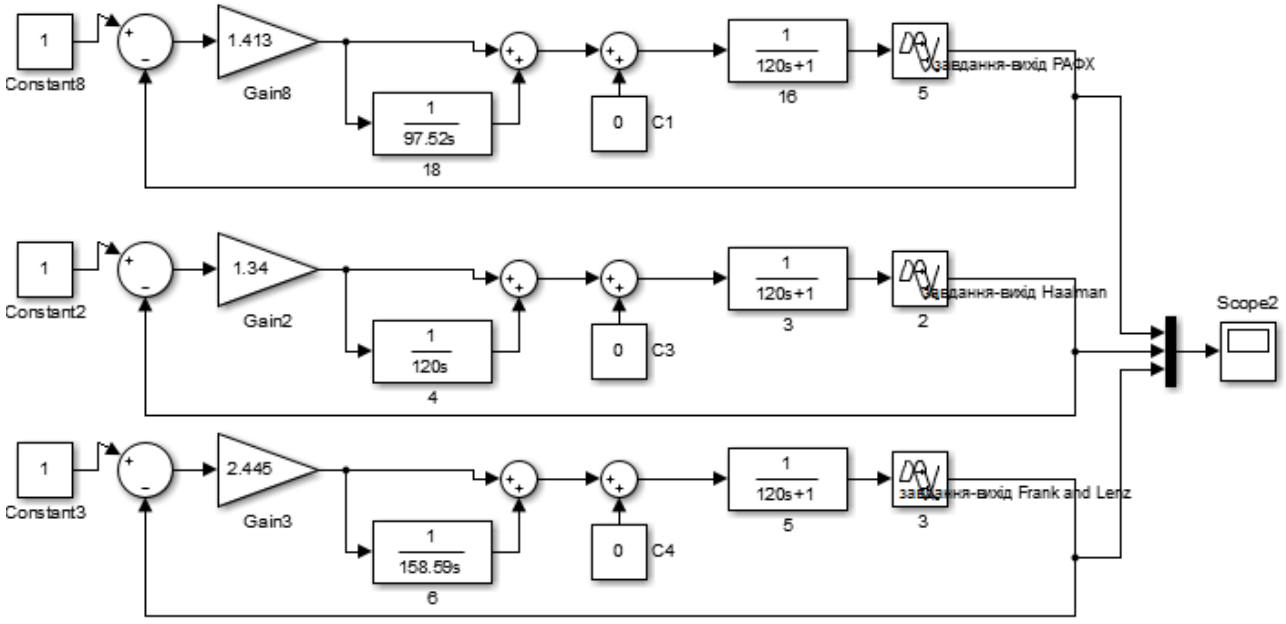


Рис. 2.7 Змодельована схема в середовищі Matlab

Результати моделювання наведені на рис.2.8 та 2.9.

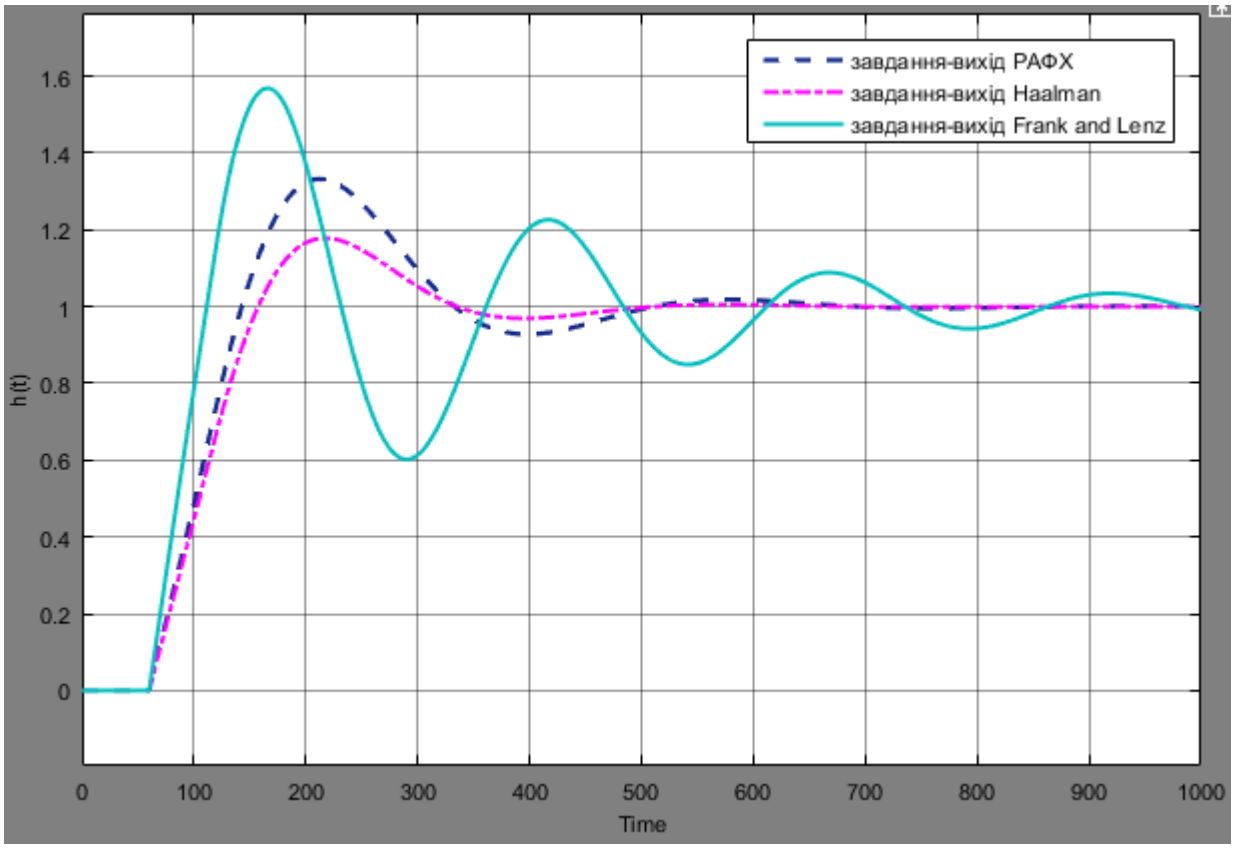


Рис. 2.8 Перехідні процеси по каналу «завдання-вихід»

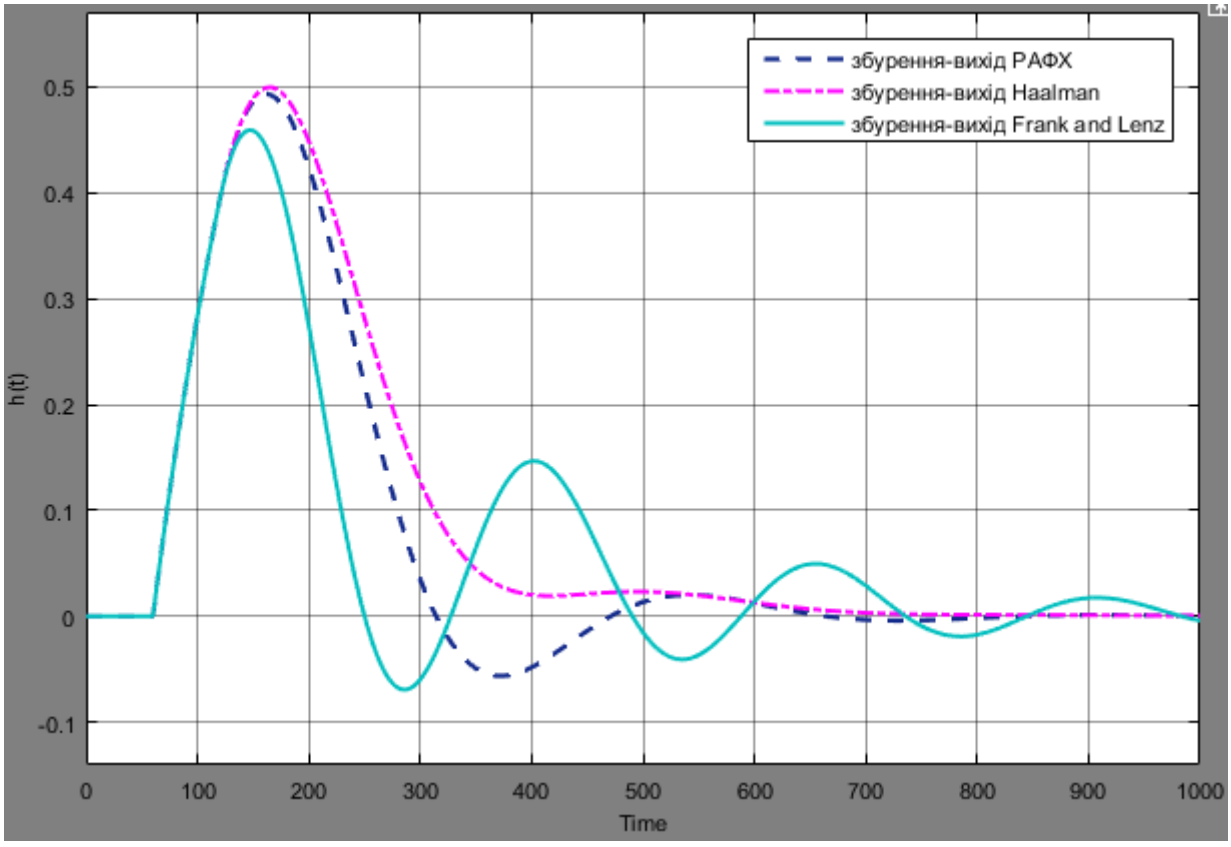


Рис.2.9 Перехідні процеси по каналу «збурення-вихід»

Розрахуємо прямі показники по каналу завдання-вихід та збурення-вихід з налаштуваннями регулятора отриманими інженерними методиками та методом РАФХ. Результати розрахунків наведені в таблиці 2.2

Таблиця 2.2 Показники якості для контуру теплового навантаження

Показник якості	«завдання-вихід»			«збурення-вихід»		
	РАФХ	Haalman	Frank and Lenz	РАФХ	Haalman	Frank and Lenz
Статична помилка $\Delta_{ст}$	0	0	0.002	0	0	0
Динамічна помилка $\Delta_{дин}$	0,332	0,178	0,5686	0,493	0,471	0,44
Степінь затухання ψ	0,94	0,97	0,60	0.96	1	0.74
Час регулювання $t_{рег}$	445	301.4	814	435	337	719
Перерегулювання σ, %	33,2	17,83	56,86	8.4	-	10.5

Порівнюючи прямі показники якості перехідних процесів з використанням різних регуляторів і враховуючи те, що для нашого об’єкта важливим критерієм є невеликий час регулювання та перерегулювання можемо зробити висновок, що ПІ-регулятор розрахований методом Haalman є оптимальнішим вибором.

2.3 КОНТУР РОЗРІДЖЕННЯ В ТОПЦІ

2.3.1 ОТРИМАННЯ ПЕРЕХІДНОЇ ХАРАКТЕРИСТИКИ

Використаємо передаточну функцію об’єкта керування теплового навантаження в твердопаливному котлі з технологічного регламенту [9]:

$$W_{об1} = \frac{0.7}{15s+1} e^{-3s}$$

$\tau_{об1} = 3c$; $T_{об1} = 15c$; $K_{об1} = 0.7 \, Па/\%ходуВМ$

Цей об’єкт належить до об’єктів з самовирівнюванням. Такий об’єкт апроксимується послідовним з’єднанням ланки транспортного запізнення та аперіодичної ланки першого порядку.[4]

2.3.2 РОЗРАХУНОК РЕГУЛЯТОРА

Для контуру регулювання розрідження в топці оберемо ПІ-закон регулювання, розрахунок параметрів регулятора виконаємо трьома методами:

1. Метод РАФХ(Розширеної амплітудно-фазової характеристики)
2. Два інженерні методи

Метод РАФХ забеспечує точність оптимізації налаштувань одноконтурних систем з типовими законами регулювання: пропорційним, інтегральним й пропорційно-інтегральним.

Обираємо для розрахунку налаштувань регулятора ступень коливальності $m = 0.45$, за якого показник затухання $\psi = 0.94$.

Скориставшись формулами для ПІ-регулятора(2.8), будуємо залежність в координатах Ki і Kp:

```
m=0.45;
w=0:0.000001:0.433;
p=-m*w+i*w;
W=(0.7*exp(-3.*p))./(15.*p+1);
Re=real(W);
Im=imag(W);
Kp=-(m.*Im+Re)./(Im.^2+Re.^2);
Ki=-w.*(m.^2+1).*Im./(Im.^2+Re.^2);
plot(Kp,Ki,'-b');
grid on;
ylabel('Ki');
xlabel('Kp');
```

Отримана крива зображена на рис 2.10. На даній криві вибираємо точку, що відповідає мінімальному інтегральному критерію якості, яка лежить справа і дорівнює $0{,}95Ki^{max} = 0{,}6723$

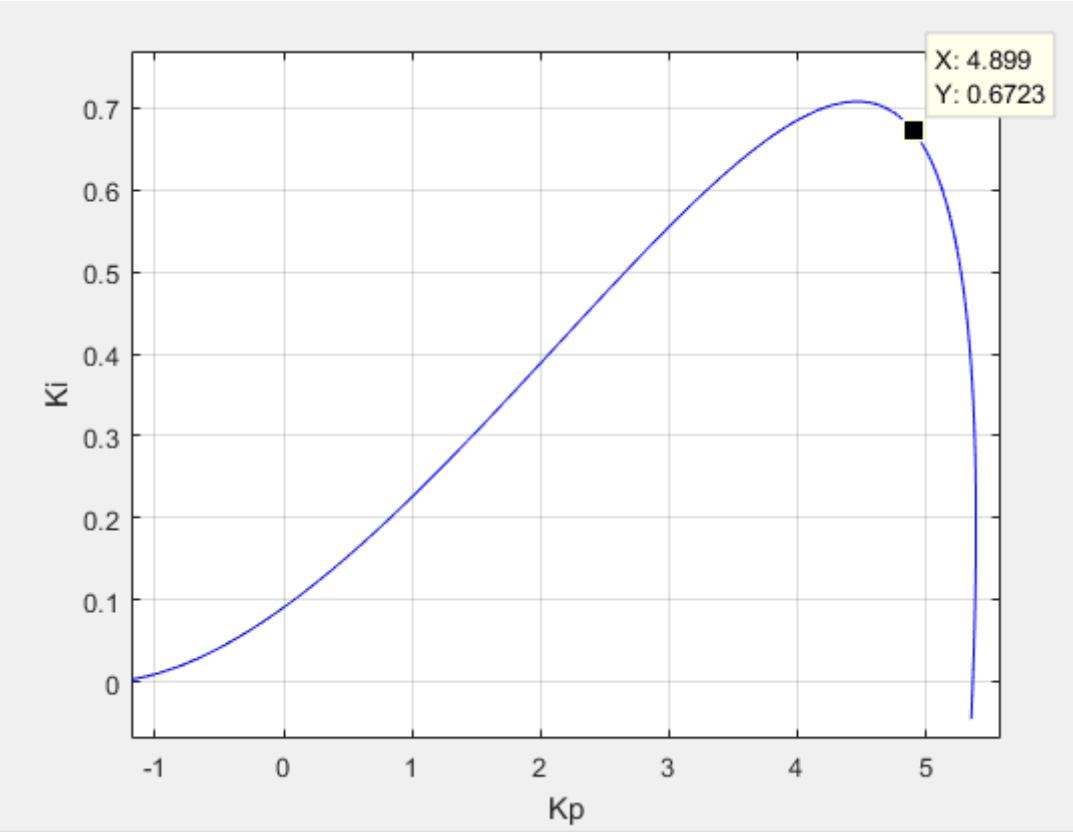


Рис.2.10 Крива налаштувань K_p , K_i контуру регулювання розрідження в топці

Таким чином параметри ПІ регулятора наступні $K_p = 4.899$, $K_\text{i} = 0.6723$, $\text{T}_\text{i} = 7{,}29$, а передаточна функція має вигляд:

Обрано інженерні методики, які так як метод РАФХ забезпечують мінімальний інтегральний критерій якості, а саме:

1. Minimum ISE - Haalman(1965): $K_p = \frac{0.67T_o}{K_o\tau_o}$, $T_i = T_o$ [7]
2. Minimum ISE - Frank and Lenz (1969): $K_p = \frac{1}{K_o}(0.53 + 0.82\frac{T_o}{\tau_o})$, $T_i = \frac{\tau_o}{0.82}(0.53 + 0.82\frac{T_o}{\tau_o})$ [7]

Розрахуємо налаштування регулятора згідно наведених методик і отримаємо:

1. $K_p = \frac{0.67*15}{0.7*3} = 4.79$, $T_i = 15$

2. $K_p = \frac{1}{0.7}(0.53 + 0.82\frac{15}{3}) = 6.61$, $T_i = \frac{3}{0.82}(0.53 + 0.82\frac{15}{3}) = 16.93$

Побудуємо перехідні процеси для замкненої САР для вибору отимальних налаштувань регулятора за допомогою пакету Matlab та розрахуємо прямі показники якості перехідного процесу по каналам «завдання – вихід» та «збурення – вихід»(рис.2.11).

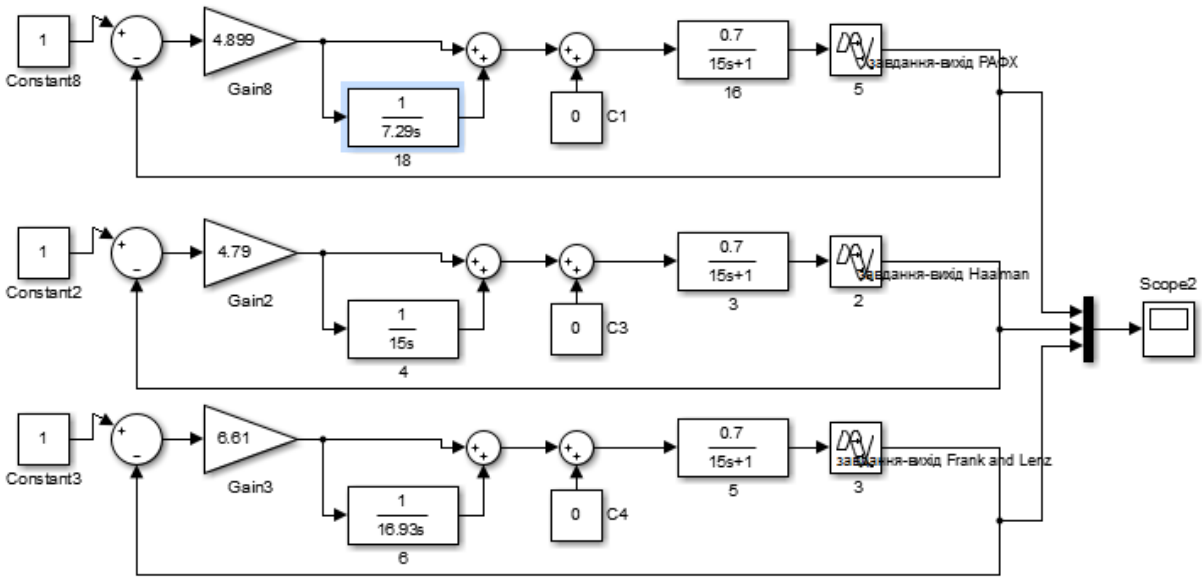


Рис. 2.11 Змодельована схема в середовищі Matlab

Результати моделювання наведені на рис.2.12 та 2.13.

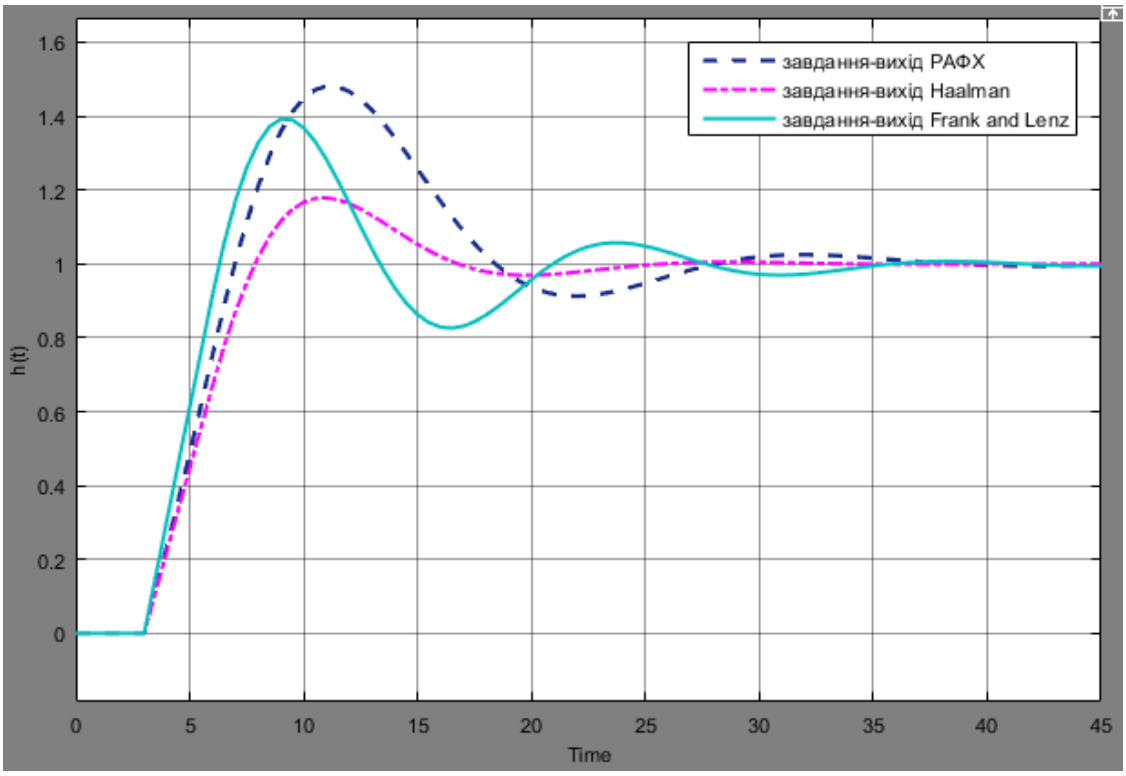


Рис. 2.12 Перехідні процеси по каналу «завдання-вихід»

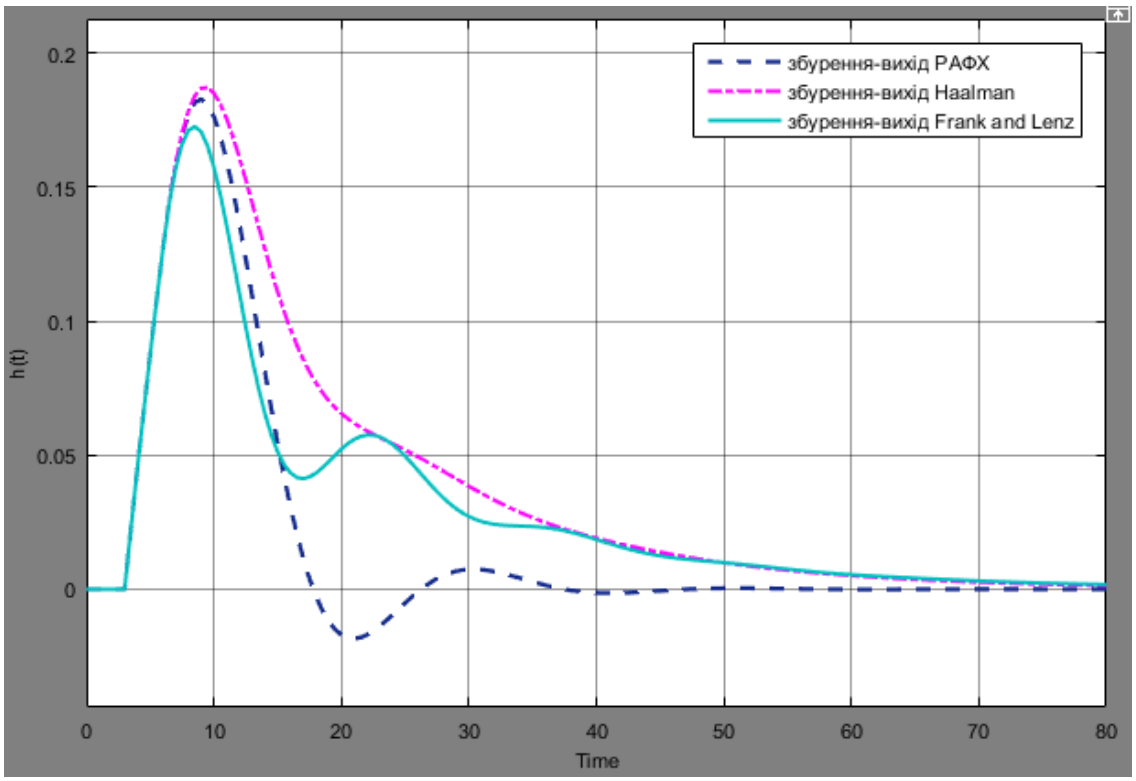


Рис.2.13 Перехідні процеси по каналу «збурення-вихід»

Розрахуємо прямі показники по каналу завдання-вихід та збурення-вихід з налаштуваннями регулятора отриманими інженерними методиками та методом РАФХ. Результати розрахунків наведені в таблиці 2.3

Таблиця 2.3 Показники якості для контуру розрідження в топці

Показник якості	«завдання-вихід»			«збурення-вихід»		
	РАФХ	Haalman	Frank and Lenz	РАФХ	Haalman	Frank and Lenz
Статична помилка $\Delta_{ст}$	0	0	0.002	0	0	0
Динамічна помилка $\Delta_{дин}$	0,481	0,1791	0,392	0,1828	0,187	0,172
Степінь затухання ψ	0,948	0,97	0,85	0,96	1	1
Час регулювання $t_{рег}$	25.1	15.1	24.8	24,1	50	52.8
Перерегулювання σ, %	48.1	17,91	39,2	9.9	-	-

Порівнюючи прямі показники якості перехідних процесів з використанням різних регуляторів і враховуючи те, що для нашого об’єкта важливим критерієм є невеликий час регулювання та перерегулювання можемо зробити висновок, що ПІ-регулятор розрахований інженерним методом Haalman є оптимальнішим вибором.

ВИСНОВКИ ДО РОЗДІЛУ 2

В розділі було проведено ідентифікацію та розрахунок налаштувань регуляторів для трьох контурів: вмісту кисню у вихідних газах, теплового навантаження, розрідження в топці котла.

Всі три об’єкти відносяться до об’єктів з самовирівнюванням і апроксимуються послідовним з’єднанням ланки транспортного запізнення та аперіодичної ланки першого порядку. В якості регуляторів було обрано Пі-регулятор, розрахунки якого здійснювався методом РАФХ, та двома інженерними методами. В результаті отримано наступні результати:

1. Контур регулювання вмісту кисню у вихідних газах:

- передаточна функція об’єкту: $W_{об1} = \frac{0,1}{27s+1} e^{-52s}$
- передаточна функція регулятора: $W_p = 3.48(\frac{27s+1}{27s})$

2. Контур регулювання теплового навантаження:
   - передаточна функція об’єкту: $W_{об1} = \frac{1}{120s+1} e^{-60s}$
   - передаточна функція регулятора: $W_p = 1.34(\frac{120s+1}{120s})$
3. Контур регулювання розрідження в топці:
   - передаточна функція об’єкту: $W_{об1} = \frac{0.7}{15s+1} e^{-3s}$
   - передаточна функція регулятора: $W_p = 4.79(\frac{15s+1}{15s})$

3. ПРОГРАМНО-ТЕХНІЧНІ РІШЕННЯ ПТКЗА

3.1 ОПИС ПРОГРАМНО-ТЕХНІЧНИХ РІШЕНЬ ЛОКАЛЬНОГО РІВНЯ ПТКЗА

Основним елементом локального рівня є програмований логічний контролер Siemens S7-300. Сигнали від давачів, зворотного зв'язку електричних приводів заводяться в контролер через модулі вводу Siemens SM331 та вбудовані входи контролера, а через модуль виводу SM334 та вбудовані виходи контроллера здійснюється керуюча дія на приводи та частотні перетворювачі. Перелік вхідних та вихідних сигналів, що задіяні на нижньому рівні, наведено у таблиці 3.1 та 3.2.

Таблиця 3.1 Вхідні сигнали

Параметр	**Діапазон**	**Точність**	**Тип сигналу**	**Призначення параметру**
Температура води на виході з котла	0-200^{0}C	0,5	Аналоговий 4-20мА	Контроль Регулювання
Температура води на вході в котел	0-200^{0}C	0,5	Аналоговий 4-20мА	Контроль
Температура в зоні горіння летких сполук	0-600^{0}C	0,5	Аналоговий 4-20мА	Контроль
Температура в зоні колосникової решітки t_2	0 - 1250^{0}C	0,5	Аналоговий 4-20мА	Контроль
Температура вихідних газів	0-200^{0}C	0,5	Аналоговий 4-20мА	Контроль
Температура на виході з котла	0-200^{0}C	0,5	Аналоговий 4-20мА	Контроль
Тиск води на виході з котла	0-1 МПа	0,ufp 5	Аналоговий 0-10 В	Контроль

Продовження таблиці 3.1

Тиск води на вході в котел	0-1 МПа	0,5	Аналоговий 0-10 В	Контроль
Розрідження в котлі	0-100Па	0,5	Аналоговий 0-10В	Контроль Регулювання
O_2 в сухих вихідних газах	0-21%	0,5	Аналоговий 4-20мА	Контроль Регулювання
Положення ВМ на клапані подачі вторинного повітря	0-100%	±0.5%	Аналоговий 0-10 В	Контроль
Положення ВМ на клапані подачі первинного повітря	0-100%	±0.5%	Аналоговий 0-10 В	Контроль
Сигнал від перетворювача частоти (дуттєвий ветрилятор)	0-100%	±0.5%	Аналоговий 0-10 В	Контроль
Сигнал від перетворювача частоти (подачі палива)	0-100%	±0.5%	Аналоговий 0-10В	Контроль
Стан роботи вентилятору подачі вторинного повітря		1	Дискретний сухий контакт 0,24В	Контроль Блокування (не працює вентилятор)
Стан роботи димососа		1	Дискретний сухий контакт 0,24В	Контроль Блокування (не працює димосос)

Таблиця 3.2 Вихідні сигнали

Регулюючий параметр	**Точність**	**Тип сигналу**	**Призначення параметру**
Керуючий сигнал на перетворювач частоти подачі палива	0,5	Аналоговий 0-10 В	Регулювання
Керуючий сигнал на перетворювач частоти електродвигуна димососа	0,5	Аналоговий 0-10 В	Регулювання
Ступінь відкриття заслінки первинного повітря	0,5	Аналоговий 0-10 В	Регулювання
Керуючий сигнал на перетворювач частоти електродвигуна вентилятора первинного повітря	0,5	Дискретний 0, 24В	Регулювання
Керуючий сигнал на перетворювач частоти електродвигуна вентилятора вторинного повітря	0,5	Дискретний 0, 24В	Регулювання
Ступінь відкриття заслінки вторинного повітря	0,5	Аналоговий 4-20мА	Регулювання
Стан роботи вентилятору подачі вторинного повітря	ввімкнений/вимкнений	Дискретний сигнал 0, 24В	Регулювання
Стан роботи димососа	ввімкнений/вимкнений	Дискретний сигнал 0, 24В	Регулювання

3.1.1 ПОРЯДОК ПРОГРАМУВАННЯ КОНТРОЛЛЕРА

Для програмування контролера використовується система програмування SIMATIC STEP 7 V 15.

Програмування контролера відбувається за наступними етапами:

1. Запуск TIA Portal V15

2. Створення нового проекту: Create new project, де можемо самі ввести назву проекту або скористатися запропонованою назвою.
3. Далі вибираємо Project viewer. У вікні Devices вибираємо Project-Devices & networks.
4. У вкладці Hardware catalog, вибираємо Catalog, де і підбираємо контролер з усіма додотковимим модулями.
5. Після встановлення налаштувань необхідно створити головну програму проекту Program blocks- Add new block. В даному діалоговому вікні здійснюється вибір мови програмування. Вибір здійснюється серед мов програмування, що визначені стандартом IEC 61131-3.
6. В залежності від вибору мови програмування відкриється відповідне вікно, в якому необхідно створити програму, що буде виконуватись на контролері.
7. Для завантаження програми в контролер необхідно вибрати Download to device, тип інтерфейсу та контролер з address яка нам необхідна. Натискаємо Load.

3.1.2 РЕАЛІЗАЦІЯ ФУНКЦІЙ НИЖНЬОГО РІВНЯ СИСТЕМИ АВТОМАТИЗАЦІЇ

1. Реалізація регулювання теплового навантаження:

- значення температури вимірюється датчиком температури Symaro-T QAE3075.010 з уніфікованим виходом 4-20 мА;
- струмовий сигнал передається на вхід контролера аналогового вводу;
- в контролері реалізована одноконтурна схема управління, регулятор – ПІ регулятор;
- контролер по шині передачі даних передає значення на модуль SM1234;
- аналоговий сигнал 4-20 мА передається на частотний перетворювач ATV-900 на вентилятор, в результаті змінюючи витрату палива;

2. Реалізація регулювання розрідження в топці котла:

- значення тиску-розрідження вимірюється в топці датчиком Symaro QBM65-1 з уніфікованим виходом 0-10 В;
- струмовий сигнал передається на вхід модуля аналогового вводу SM1234;
- в контролері реалізована одноконтурна схема управління, регулятор – ПІ регулятор;
- контролер передає аналоговий сигнал 4-20 мА на частотний перетворювач ATV900;
- змінюється частота обертання двигуна димососа, змінюємо розрідження в топці котла.

3. Реалізація регулювання вмісту кисню у вихідних газах:

- значення концентрації кисню в димових газах вимірюється газоаналізатором Siemens OXYMAT6 з вихідним унівікованим синалом 4-20 мА;
- струмовий сигнал передається на вхід модуля аналогового вводу SM1234;
- в контролері реалізована одноконтурна схема управління, регулятор – ПІ регулятор;
- контролер передає аналоговий сигнал 4-20 мА на електропривід заслінки АNТЗ-11.11;
- виконавчий механізми змінюють витрату подачі повітря.

3.1.3 РУЧНЕ УПРАВЛІННЯ ТЕХНОЛОГІЧНИМ ПРОЦЕСОМ

Реалізація ручного керування здійснюється за допомогою HMI-панелі TP900 Comfort марки Siemens, де присутня можливість задавати керуючий вплив заслінці та частотним перетворювачам .

3.2 ОПИС ПРОГРАМНО-ТЕХНІЧНИХ РІШЕНЬ СУПЕРВІЗОРНОГО РІВНЯ ПТКЗА

3.2.1 ПОРЯДОК СТВОРЕННЯ SCADA-ПРОГРАМИ, ТА ВЗАЄМОДІЯ З НИЖНІМ РІВНЕМ АВТОМАТИЗАЦІЇ

Супервізорний рівень системи керування являє собою SCADA-систему. SCADA-система в даній роботі реалізує відображання мнемосхем технологічного процесу та значень технологічних параметрів, виконує реєстрацію спрацювання технологічної сигналізації, обмін даними з контролером.

Для створення SCADA-системи використовуємо середовище розробки WinCC.

Програмний комплекс SIMATIC Windows Control Center (WinCC) представляє необхідні засоби для керування процесами. Ця програмна область дозволяє створювати звіти, реєструвати значення вимірюючих величин, фіксувати і архівувати дані, керувати користувачами та правами їх доступу. Також середовище підтримує постійний контроль якості, тобто відбувається контролювання і слідкування, змінювання кожної операції та події. Окрім того SIMATIC WinCC містить в собі широкий асортимент бібліотеки, засоби для обробки масивів даних, зручний об’єктно-орієнтований графічний модуль з індивідуальними налаштуваннями. Передбачена можливість внесення оперативних змінних в проект, в online-режимі та взаємодія з комплексом SIMATIC Step 7.

Програмне забезпечення дає ряд унікальних інтерфейсів та редакторів, які використовуються для персонального визначення можливостей проекта. Основні з них:

- Редактор кадрів процесів та діалогових вікон WinCC Graphics Designer;
- Конфігурація системи архівування WinCC Tag Logging;
- Модуль системи оперативних та аварійних повідомлень WinCC Alarm Logging.

SCADA-програма складається з таких діалогових вікон з необхідними елементами навігації, відображення та зберігання параметрів технологічного процесу:

1. Вікно мнемосхеми котла – вікно із схематичним зображенням технологічного об’єкту управління в цілому та значень технологічних параметрів, з можливістю відслідковування спрацювання аварій та переходами на мнемосхеми регулювання кожного з контурів окремо.

2. Вікно мнемосхеми регулювання теплового навантаження – що має містити вікно трендів технологічного процесу, можливість задання параметрів уставки, параметрів регулятора та керуючи вплив.

3. Вікно мнемосхеми регулювання вмісту кисню у вихідних газах – що має містити вікно трендів технологічного процесу, можливість задання параметрів уставки, параметрів регулятора та керуючи вплив.

4. Вікно мнемосхеми регулювання розрідження в топці – що має містити вікно трендів технологічного процесу, можливість задання параметрів уставки, параметрів регулятора та керуючи вплив.

3.3 ОПИС ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯЛОКАЛЬНОГО РІВНЯ ПТКЗА

Програмне забезпечення локального рівня було розроблене у середовищі TIA Portal V15, яке включає програмне забезпечення для HMI-панелі та контролера. Програма містить наступні блоки, які зображені на рис.3.1

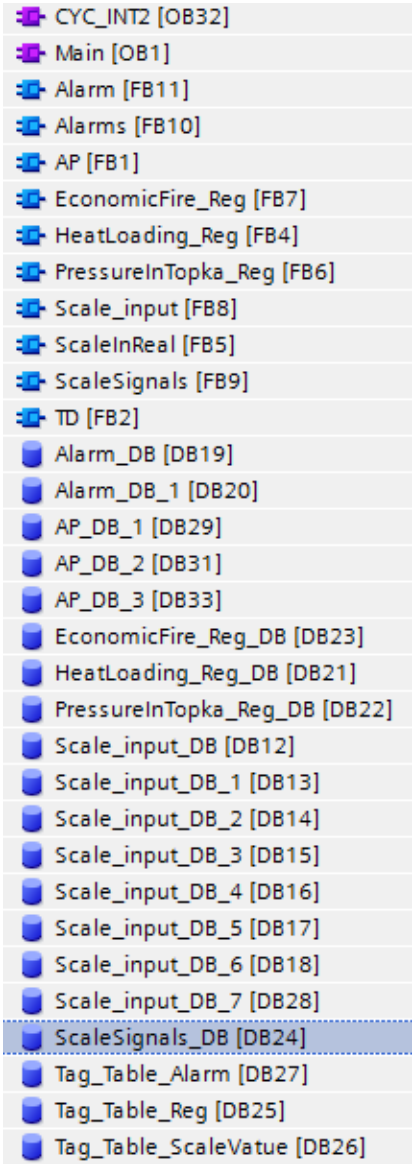


Рис. 3.1 Блоки, які містить програма

Організаційний блок CYC_INT2 потрібний для ініціалізації та запуску блоків(Alarms, ScaleSignals, EconomicFire_Reg, HeatLoading_Reg, PressureInTopka_Reg). Структуру блоку зображено на рис. 3.2-3.3

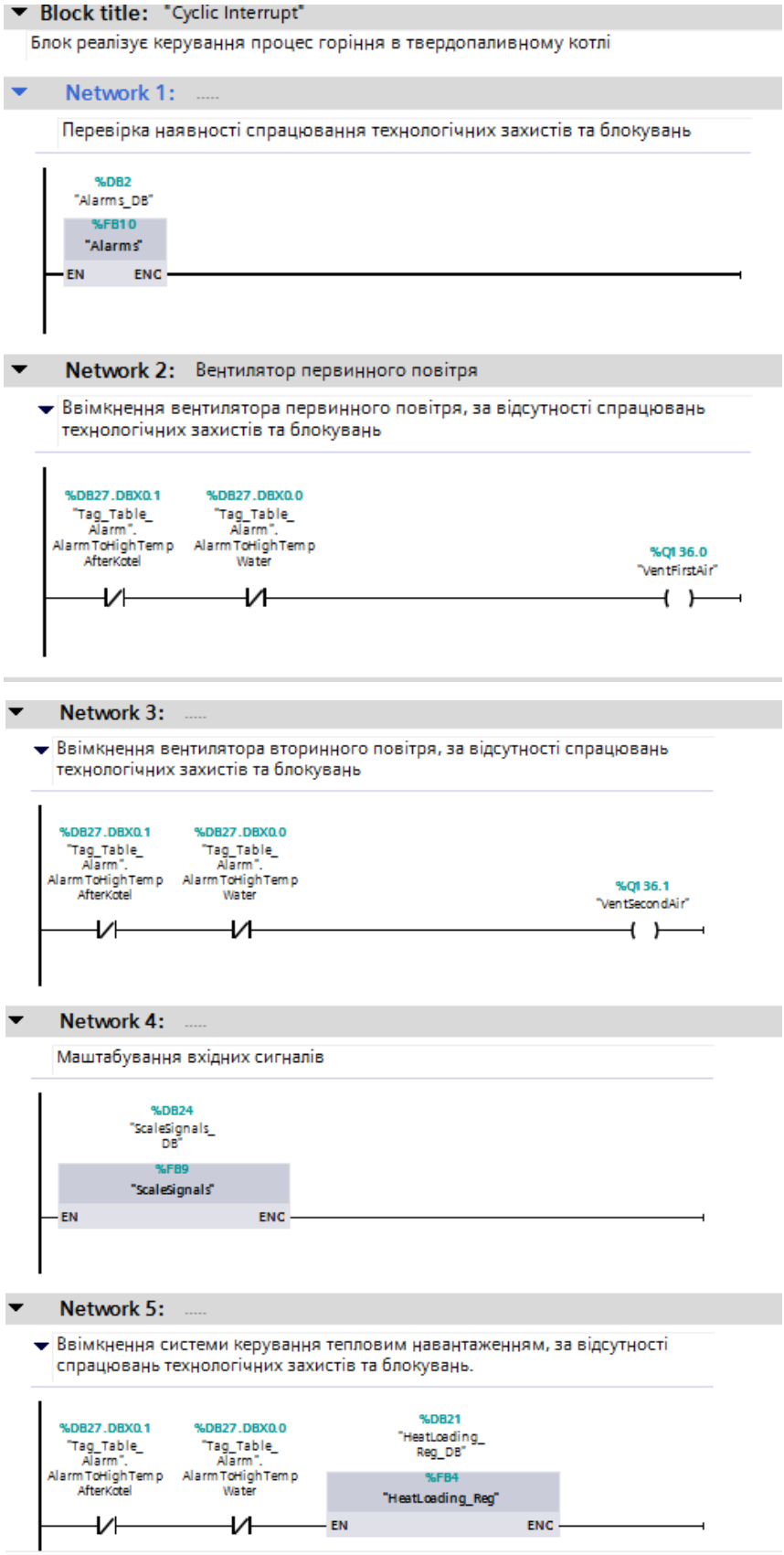


Рис. 3.2 Структура організаційного блоку CYC_INT5

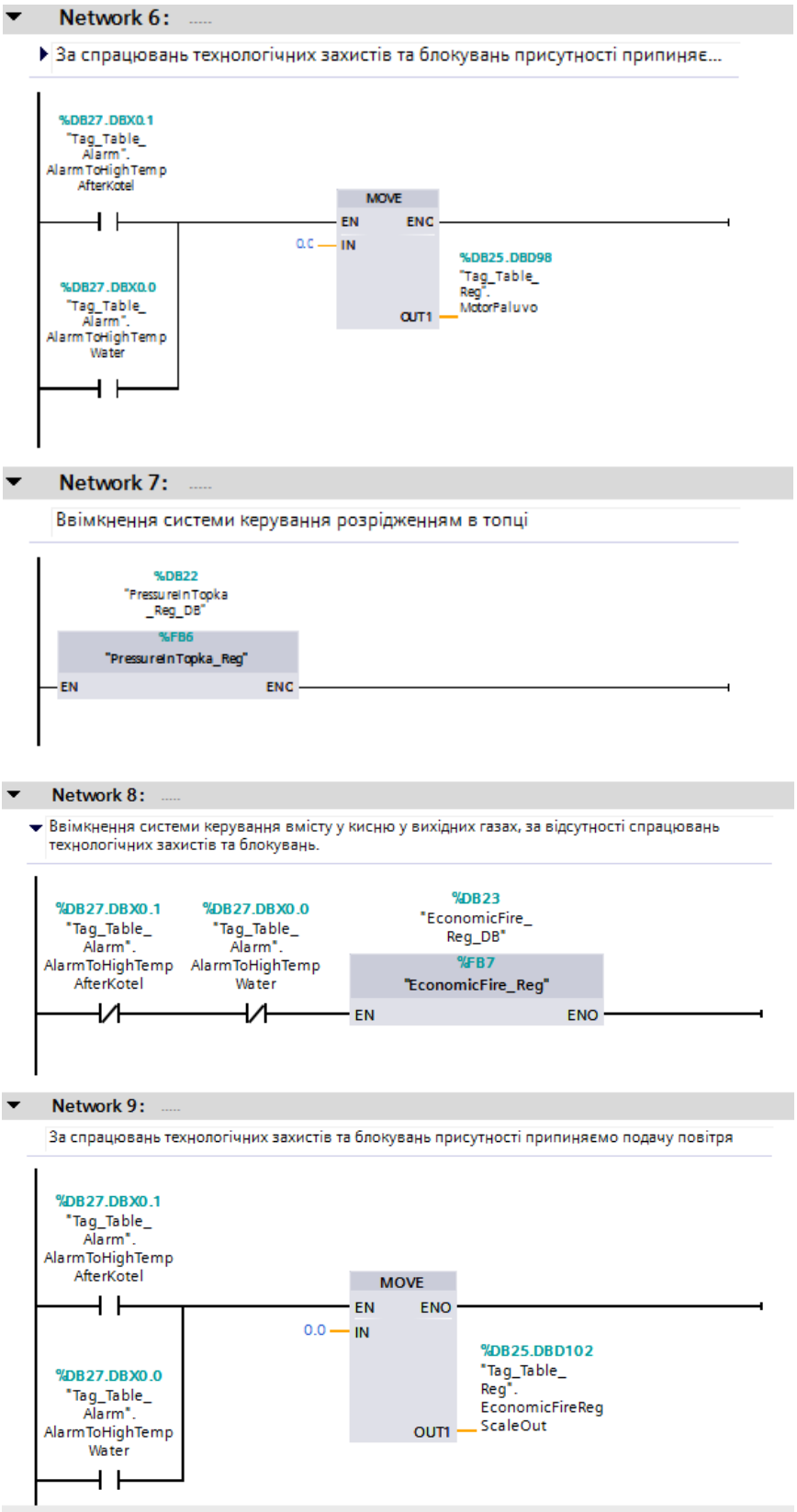


Рис. 3.3 Продовження структури організаційного блоку CYC_INT5

Функціональні блоки EconomicFire_Reg, HeatLoading_Reg, PressureInTopka_Reg (рис. 3.4-3.10) реалізовують контури регулювання вмісту кисню у вихідних газах, теплового навантаження та розрідження в топці. У блоках

використовуються глобальні змінні прописані у блоці Tag_Table_Reg. Блок EconomicFire_Reg, HeatLoading_Reg запускаються лишень у випадку відсутності технологічних захистів та блокування.

Tag_Table_Reg

	Name	Data ...	Offset	Start value	Reta...	Visi...	...	Comment
1	Static							
2	SetPointHeatLoding	Real	0.0	0.0	☑	☑	☐	Уставка температури в контурі керування теплового навантаження
3	ManualValueHeatLoding	Real	4.0	0.0	☑	☑	☐	Вплив ручного керування в контурі керування теплового навантаження
4	ManualModeHeatLoding	Bool	8.0	false	☑	☑	☐	Ввімкнення ручного режиму в контурі керування теплового навантаження
5	TemperatureHotWaterReg	Real	10.0	0.0	☑	☑	☐	температура гарячої води в контурі керування теплового навантаження
6	SetPointPressureInTopka	Real	14.0	0.0	☑	☑	☐	Уставка тиску в контурі керування розрідження в топці
7	ManualValuePressureInTopka	Real	18.0	0.0	☑	☑	☐	Вплив ручного керування в контурі керування розрідження в топці
8	ManualModePressureInTopka	Bool	22.0	false	☑	☑	☐	Ввімкнення ручного режиму в контурі керування розрідження в топці
9	PressureInTopkaReg	Real	24.0	0.0	☑	☑	☐	Розрідження в топці в контурі керування розрідження в топці
10	KpHeatLoading	Real	28.0	1.34	☑	☑	☐	Налаштування регулятора Kp в контурі керування розрідження в топці
11	KpPressureInTopka	Real	32.0	4.79	☑	☑	☐	Налаштування регулятора Kp в контурі керування розрідження в топці
12	TIKpPressureInTopka	Time	36.0	T#15s	☑	☑	☐	Налаштування регулятора Ti в контурі керування розрідження в топці
13	TdKpPressureInTopka	Time	40.0	T#0ms	☑	☑	☐	Налаштування регулятора Td в контурі керування розрідження в топці
14	TiHeatLoading	Time	44.0	T#120s	☑	☑	☐	Налаштування регулятора Ti в контурі теплового навантаження
15	TdHeatLoading	Time	48.0	T#0ms	☑	☑	☐	Налаштування регулятора Td в контурі теплового навантаження
16	SetPointEconomicFire	Real	52.0	0.0	☑	☑	☐	Уставка вмісту O2 в контурі керування вмісту кисню у вихідних газах
17	ManualValueEconomicFire	Real	56.0	0.0	☑	☑	☐	Вплив ручного керування в контурі керуванняvмісту кисню у вихідних газах
18	O2InFuelGases	Real	60.0	0.0	☑	☑	☐	Розрідження в топці
19	KpEconomicFire	Real	64.0	3.48	☑	☑	☐	Налаштування регулятора Kp в контурі керування вмісту кисню у вихідних га...
20	ManualModeEconomicFire	Bool	68.0	false	☑	☑	☐	Ввімкнення ручного режиму в контурі керуванняvмісту кисню у вихідних газ...
21	TiEconomicFire	Time	70.0	T#27s	☑	☑	☐	Налаштування регулятора Ti в контурі керування вмісту кисню у вихідних газ...
22	TdEconomicFire	Time	74.0	T#0ms	☑	☑	☐	Налаштування регулятора Td в контурі керування вмісту кисню у вихідних га...
23	MotorDutev	Real	78.0	0.0	☑	☑	☐	Сигнал на частотний перетворювач дутєвого вентилятора
24	Zaslink2	Real	82.0	0.0	☑	☑	☐	Заслінка вторинного повітря 2
25	Zaslink3	Real	86.0	0.0	☑	☑	☐	Заслінка вторинного повітря 3
26	ZaslinkaFirst	Real	90.0	0.0	☑	☑	☐	Заслінка первинного повітря
27	Zaslink1	Real	94.0	0.0	☑	☑	☐	Заслінка вторинного повітря 1
28	MotorPaluvo	Real	98.0	0.0	☑	☑	☐	Сигнал на частотний перетворювач подачі палива
29	EconomicFireRegScaleOut	Real	102.0	0.0	☑	☑	☐	Вихід регулятора в контурі керування економічності горіння

Рис. 3.4 База даних глобальних змінних

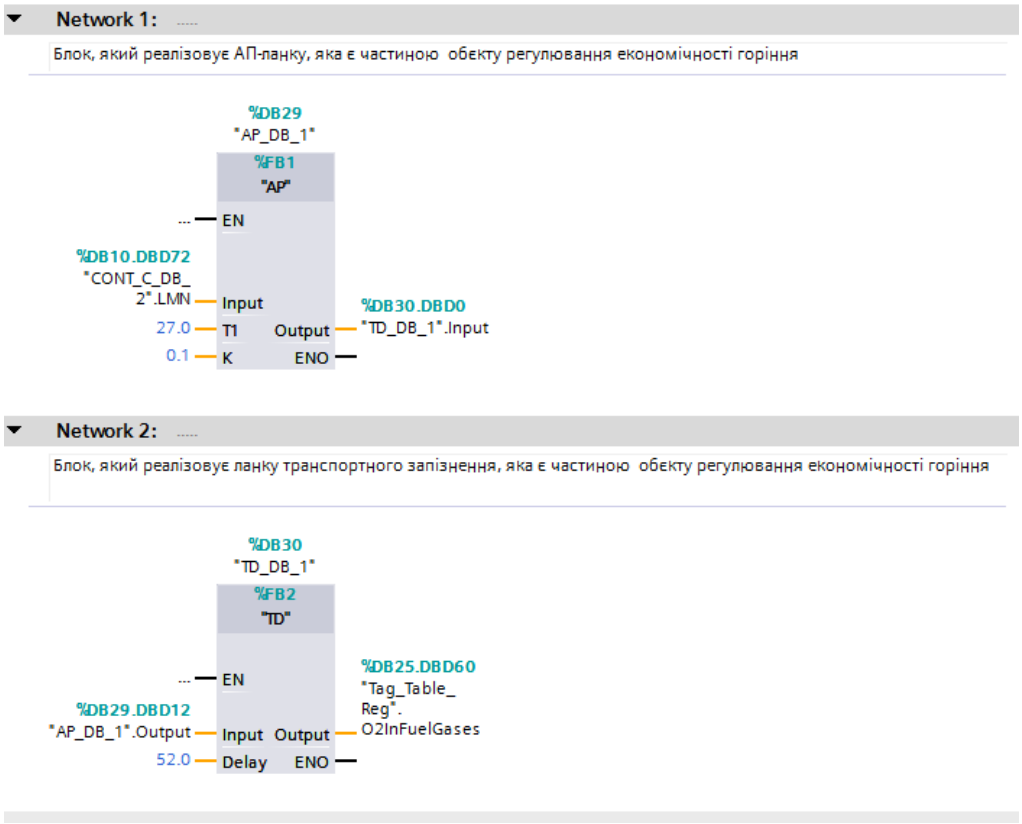


Рис. 3.5 Структура блоку EconomicFire_Reg

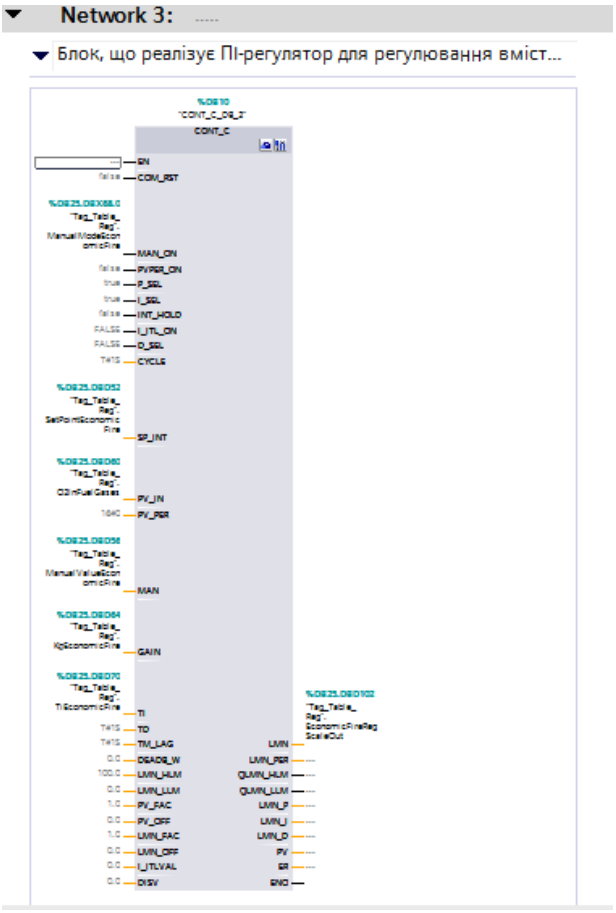


Рис. 3.6 Продовження структури блоку EconomicFire_Reg

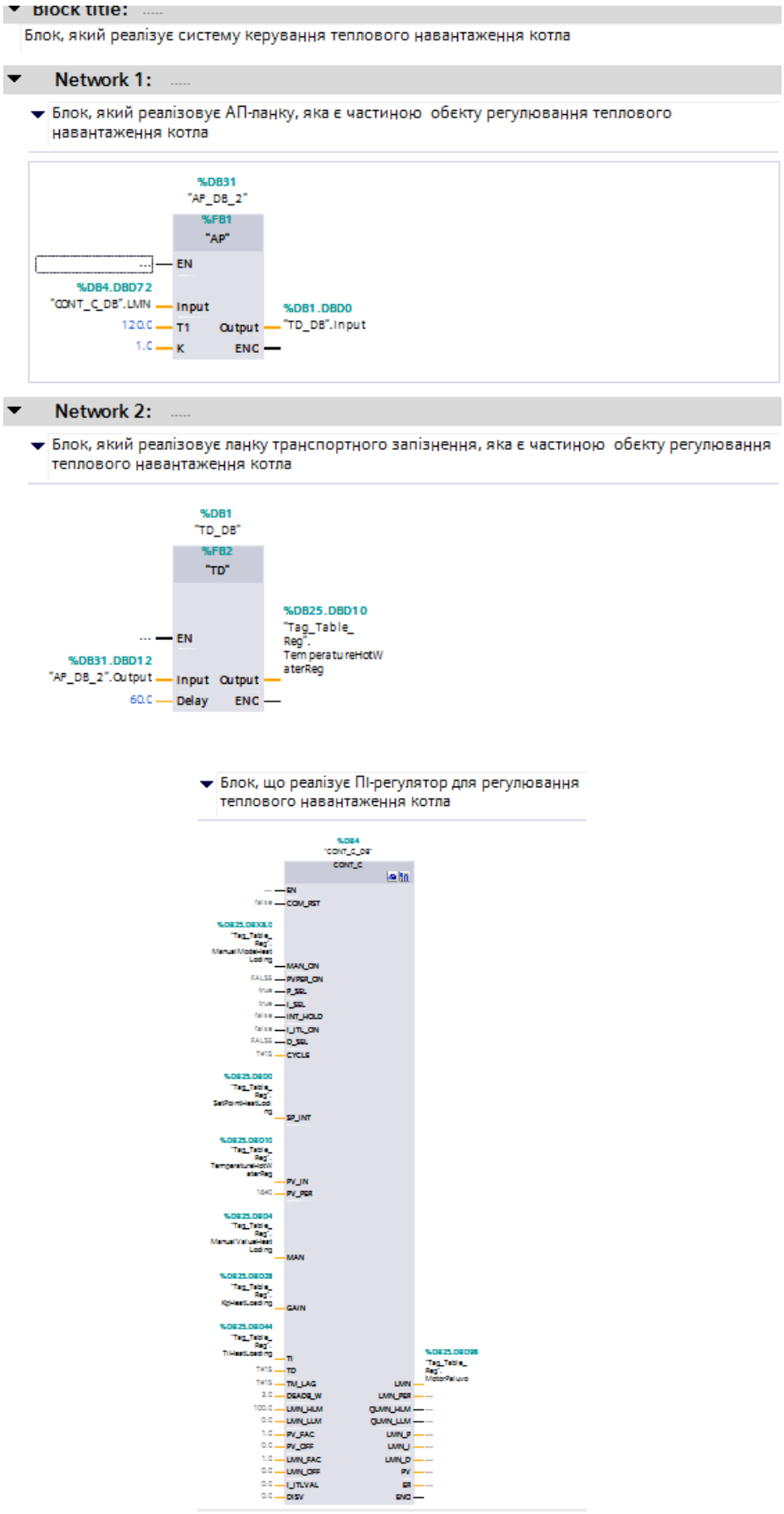


Рис. 3.7 Структура блоку HeatLoading_Reg

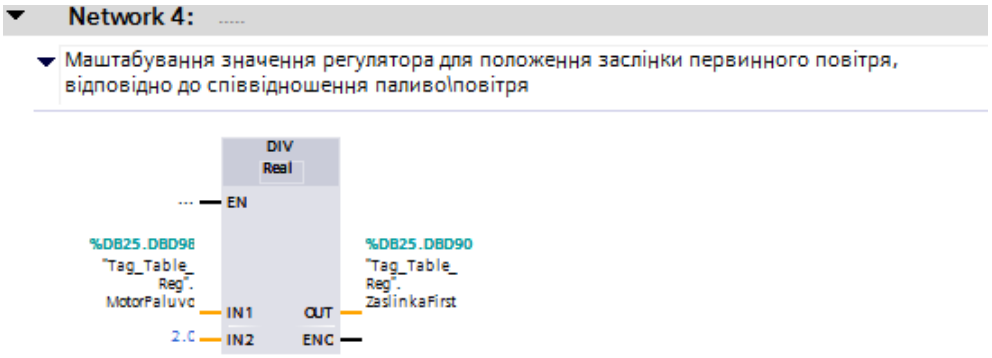


Рис. 3.8 Продовження структури блоку HeatLoading_Reg

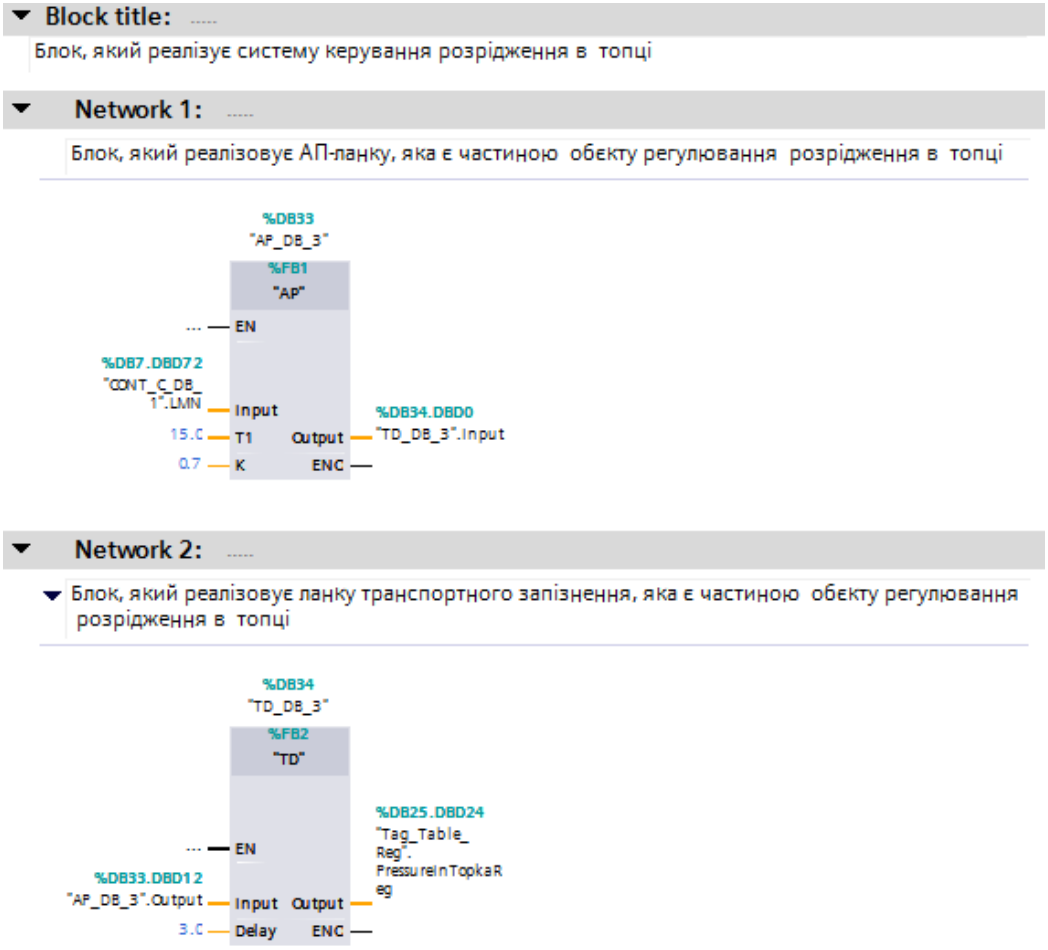


Рис. 3.9 Структура блоку PressureInTopka_Reg

Рис. 3.10 Продовження структури блоку PressureInTopka_Reg

Функціональний блок Signal_input(рис.3.11-3.12), потрібний для перетворення сигналів від контроллера у маштабовані сигнали, які відповідають шкалі наших датчиків.

	Input						
	Input	Int	0.0	0	☑	☐	Вхідний сигнал
	Low_In	Real	2.0	0.0	☑	☐	Нижня межа
	Hihg_In	Real	6.0	0.0	☑	☐	Верхня межа
	K	Real	10.0	0.0	☑	☐	Коефіцієнт підсилення
	Output				☐	☐	
	Output	Real	14.0	0.0	☑	☐	Вихідний сигнал
	err	Word	18.0	16#0	☑	☐	Помилка

Рис. 3.11 Локальні змінні функціонального блоку Signal_input

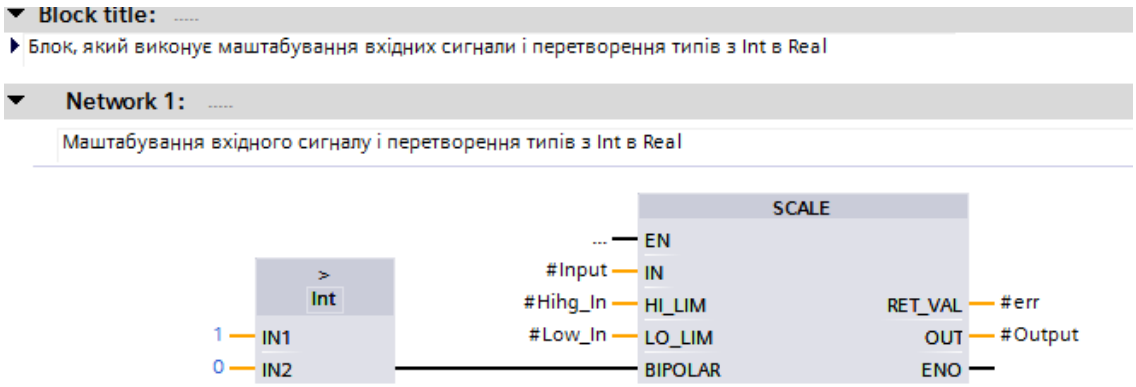


Рис. 3.12 Структура блоку Signal_input

У блоці ScaleSignals(рис.3.13-3.15) ми безпосередньо масштабуємо фізичні входи до шкали датчиків.

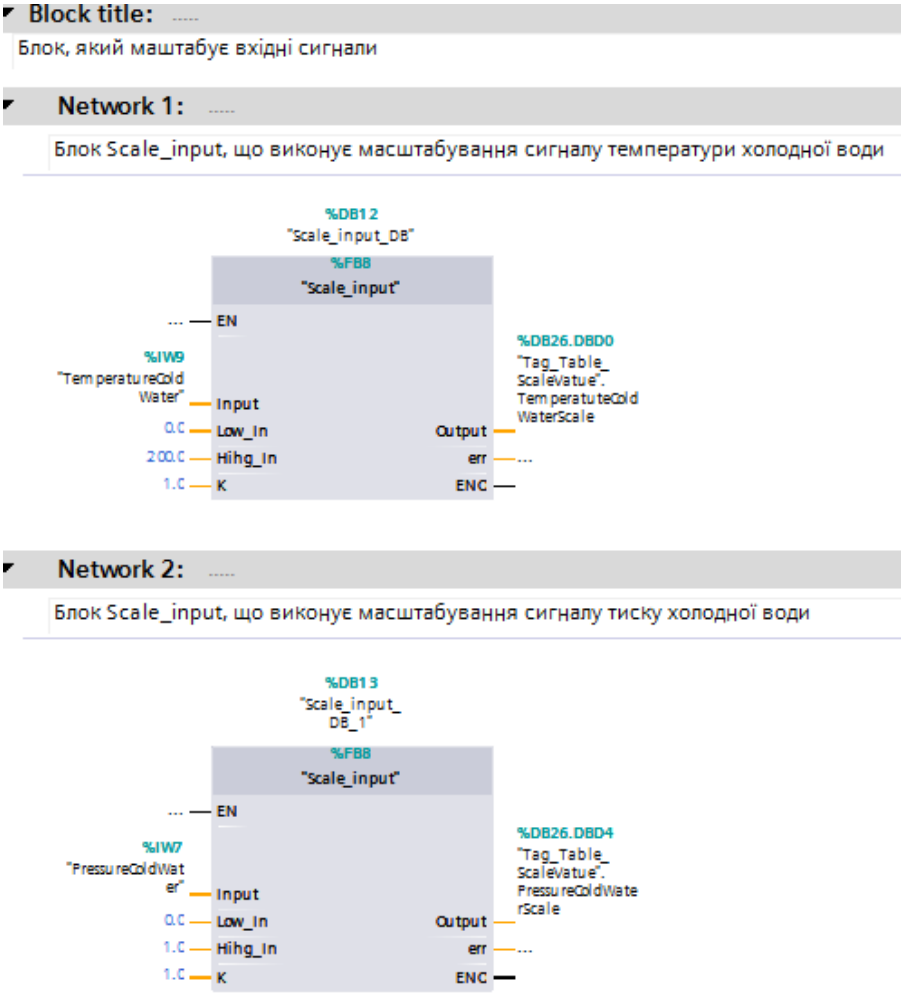


Рис. 3.13 Структура блоку ScaleSignals

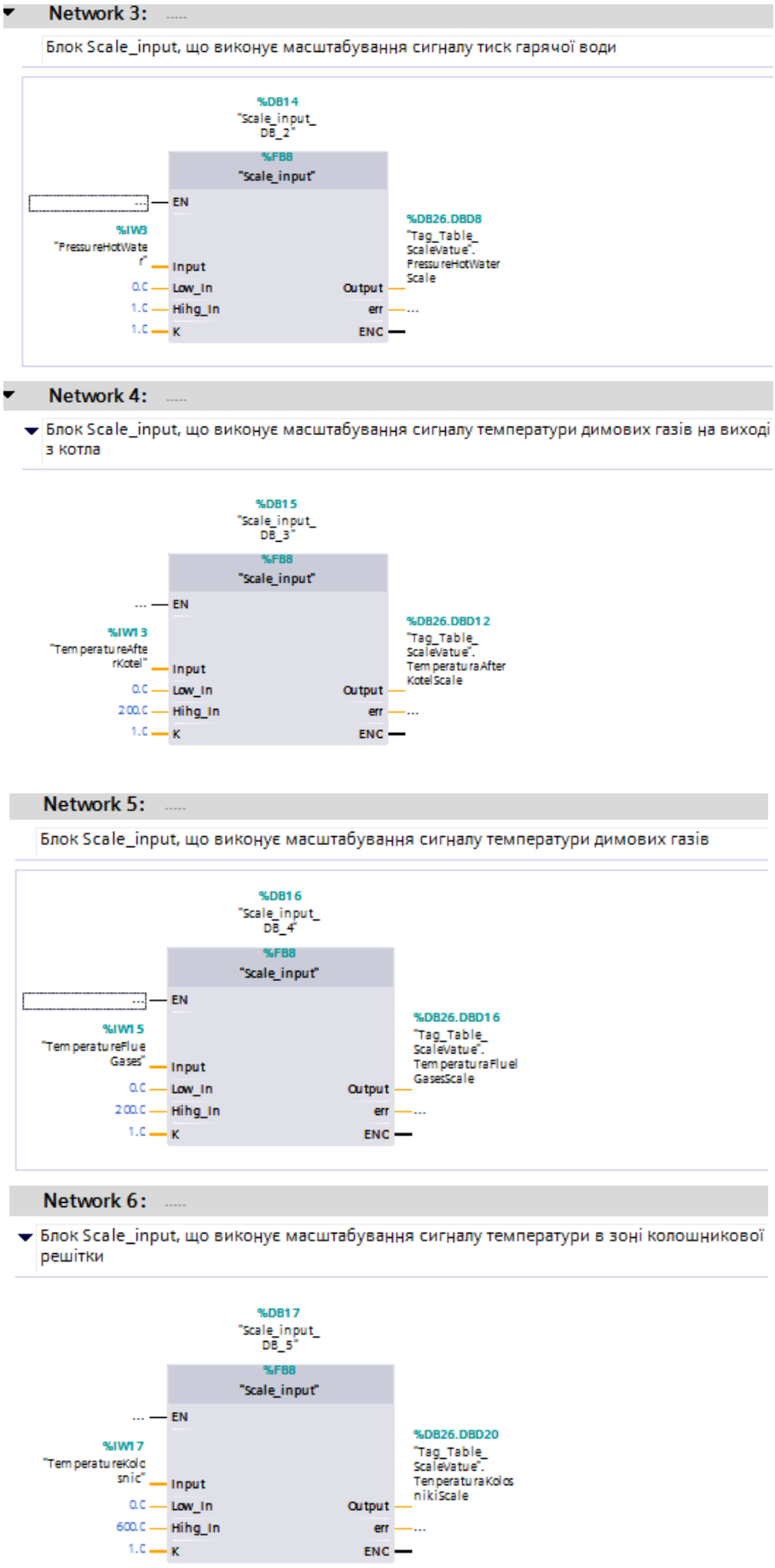


Рис. 3.14 Продовження структури блоку ScaleSignals

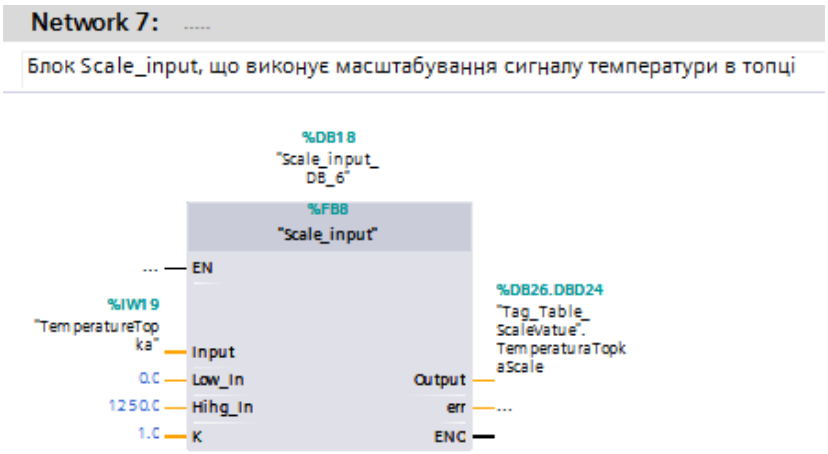


Рис. 3.15 Продовження структури блоку ScaleSignals

Захисна функція та блокування реалізовано за допомогою блоків Alarm(рис.3.16-3.17) і Alarms(рис. 3.18), у них порівнюються значення технологічних параметрів із критичними значеннями, у разі досягнення яких вмикається технологічний захист та блокування.

	Input						
	Input	Real	0.0	0.0	☑	☐	Вхідний сигнал, який порівнюється з...
	Limit	Real	4.0	0.0	☑	☐	Значення обмеження
	Output				☐	☐	
	Status	Bool	8.0	false	☑	☐	Змінна відображає статус аварії

Рис. 3.16 Локальні змінні функціонального блоку Alarm

```
1  (*Перевірка умови ввімкнення сигналізації і її задання*)
2  IF (#Input >= #Limit) THEN
3      #Status := TRUE;
4  ELSE
5      #Status := FALSE;
6  END_IF;
```

Рис. 3.16 Структура блоку Alarm

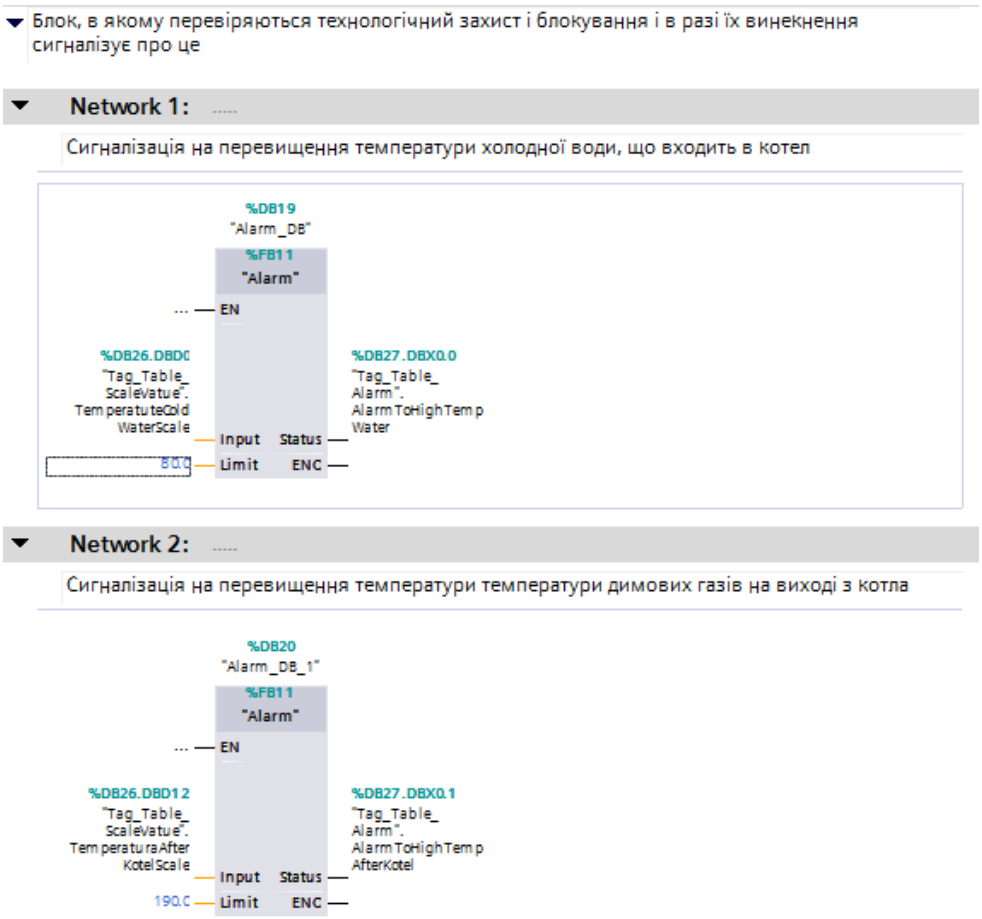


Рис. 3.16 Структура блоку Alarms

Блок Tag_Table_Scale (рис.3.17) містить глобальні змінні, які використовуються в блоці ScaleSignals та Робочою станцією.

Tag_Table_ScaleVatue

Name	Dat...	Of...	St...	Ret...	Vi...	Se...	Comment
Static							
TemperatuteColdWate...	...	0.0	0.0	☑	☑	☐	Відмаштабований сигнал від датчика температури холодної води
PressureColdWaterScale	Real	4.0	0.0	☑	☑	☐	Відмаштабований сигнал від датчика тиску холодної води
PressureHotWaterScale	Real	8.0	0.0	☑	☑	☐	Відмаштабований сигнал від датчика температури гарячої води
TemperaturaAfterKote...	Real	12.0	0.0	☑	☑	☐	Відмаштабований сигнал від датчика температури димових газів на виході з котла
TemperaturaFluelGase...	Real	16.0	0.0	☑	☑	☐	Відмаштабований сигнал від датчика температури димових газів
TenperaturaKolosnikiS...	Real	20.0	0.0	☑	☑	☐	Відмаштабований сигнал від датчика температури в зоні колосникової решітки
TemperaturaTopkaScale	Real	24.0	0.0	☑	☑	☐	Відмаштабований сигнал від датчика температури в топці котла

Рис. 3.17 База даних Tag_Table_Scale глобальних змінних

Блок Tag_Table_Scale (рис.3.18) містить глобальні змінні, які використовуються в блоці Alarms та Робочою станцією.

Tag_Table_Alarm

Name	Data t...	O...	S...	Ret...	Vis...	S...	Comment
Static							
AlarmToHighTempWater	Bool	0.0	fals	☑	☑	☐	Змінна сигналізує про винекнення технологічного блокування при перевищенні температури холодної води, яка входить в котел
AlarmToHighTempAfterKotel	Bool	0.1	fals	☑	☑	☐	Змінна сигналізує про винекнення технологічного блокування при перевищенні температури димових газів на виході із котла

Рис. 3.18 База даних Tag_Table_Scale глобальних змінних

Узгодження режиму роботи із верхнім рівнем системи автоматизації організована наступним чином:

- Оператор може в ручному режимі має можливість змінити положення регулюючих органів.
- Оператор може в автоматичному режимі має можливість змінити завдання для кожної із систем.
- У верхній рівень відбувається передача значень необхідних змінних.

3.4 ОПИС ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ СУПЕРВІЗОРНОГО РІВНЯ ПТКЗА

Програмне забезпечення верхнього рівня системи автоматизації представлене у вигляді SCADA-програми. Вона включає наступні вікна: вікно з мнемосхемою котла, вікно регулювання теплового навантаження в котлі, вікно регулювання вмісту кисню у вихідних газах та вікно регулювання розрідження в топці.

Після запуску з’являється мнемосхема котла (рис.3.19) із кнопками переходу на вище вказані мнемосхеми, індикація контрольованих параметрів котла, а також вікно з аваріями та індикація наявності виникнення технологічних захистів та блокування.

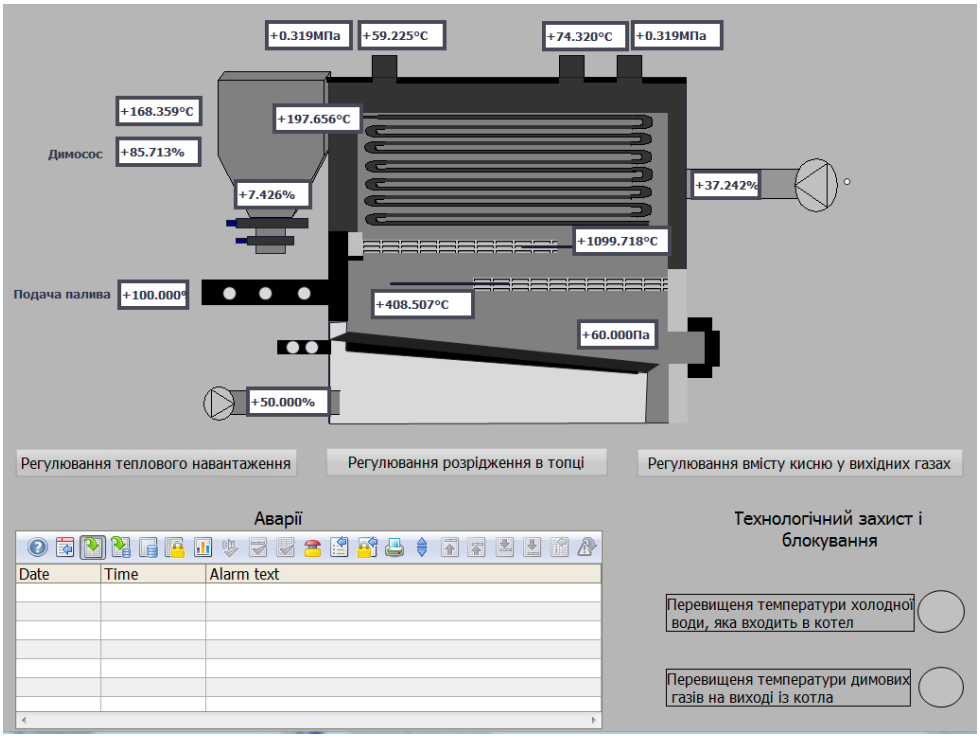


Рис. 3.19 Вікно мнемосхеми котла

Вікно регулювання теплового навантаження в котлі(рис.3.20) містить індикацію параметру, який регулюється; сигнал, який подається на ВМ; можливість задати уставку; перемкнути режими робота та подати керуючий вплив; змінити налаштування регулятора; побачити тренд з параметром, який регулюється. При ввімкненні Ручного режиму кнопка Авт/Руч жовтим кольором.

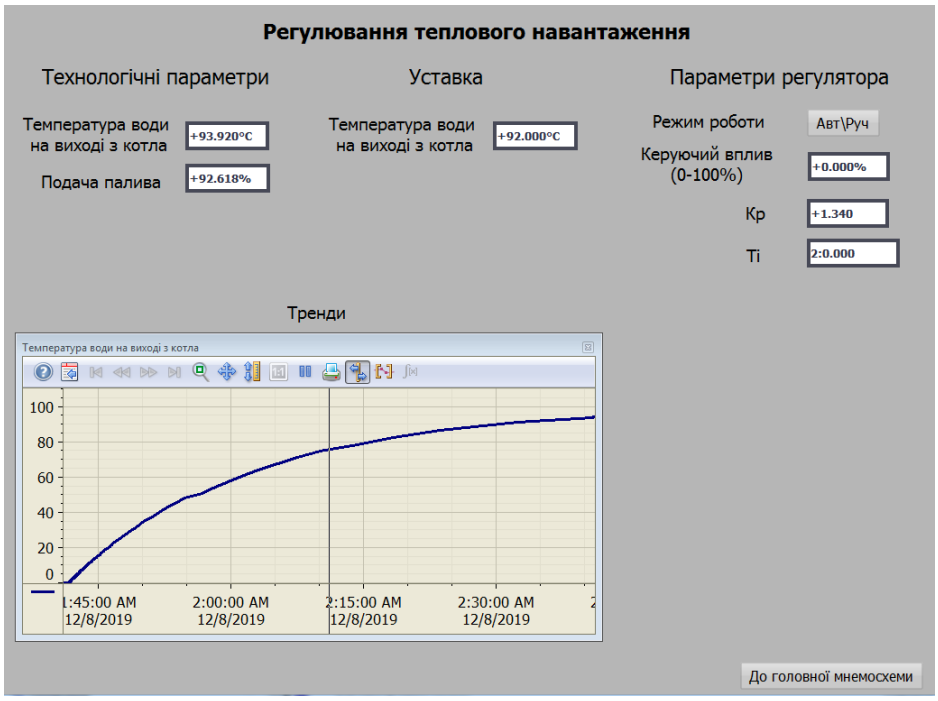


Рис. 3.20 Вікно регулювання теплового навантаження

Вікно регулювання вмісту кисню у вихідних газах на виході з котла(рис. 3.21) містить індикацію параметру, який регулюється; сигнал, який подається на ВМ; можливість задати уставку; перемкнути режими робота та подати керуючий вплив; змінити налаштування регулятора; побачити тренд з параметром, який регулюється. При ввімкненні Ручного режиму кнопка Авт/Руч жовтим кольором.

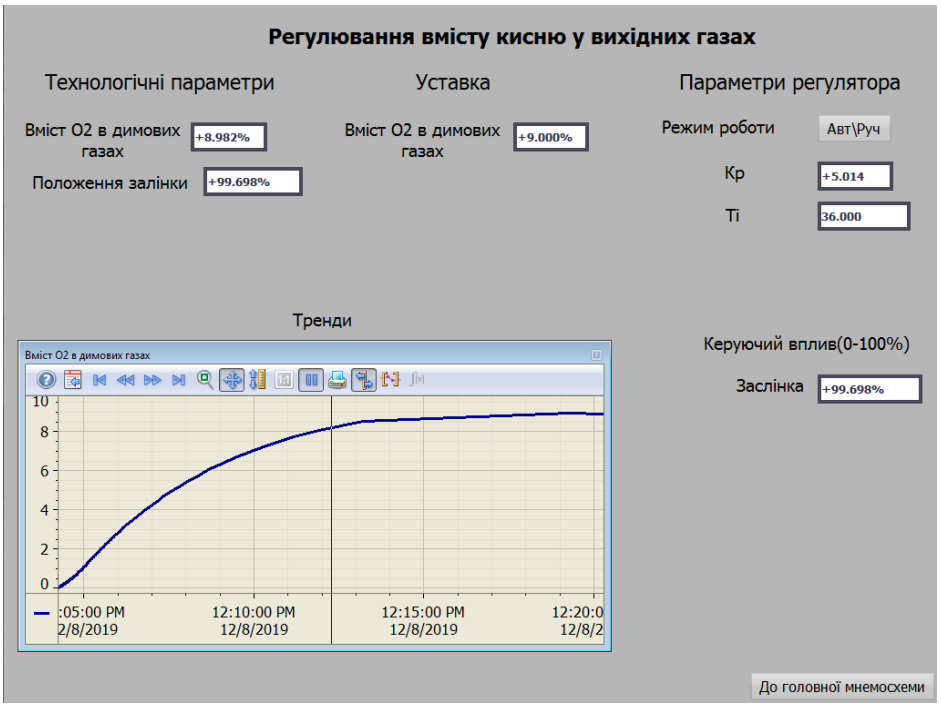


Рис. 3.21 Вікно регулювання вмісту кисню у вихідних газах

Вікно регулювання розрідження в топці в котлі(рис. 3.22) містить індикацію параметру, який регулюється; сигнал, який подається на ВМ; можливість задати уставку; перемкнути режими робота та подати керуючий вплив; змінити налаштування регулятора; побачити тренд з параметром, який регулюється. При ввімкненні Ручного режиму кнопка Авт/Руч жовтим кольором.

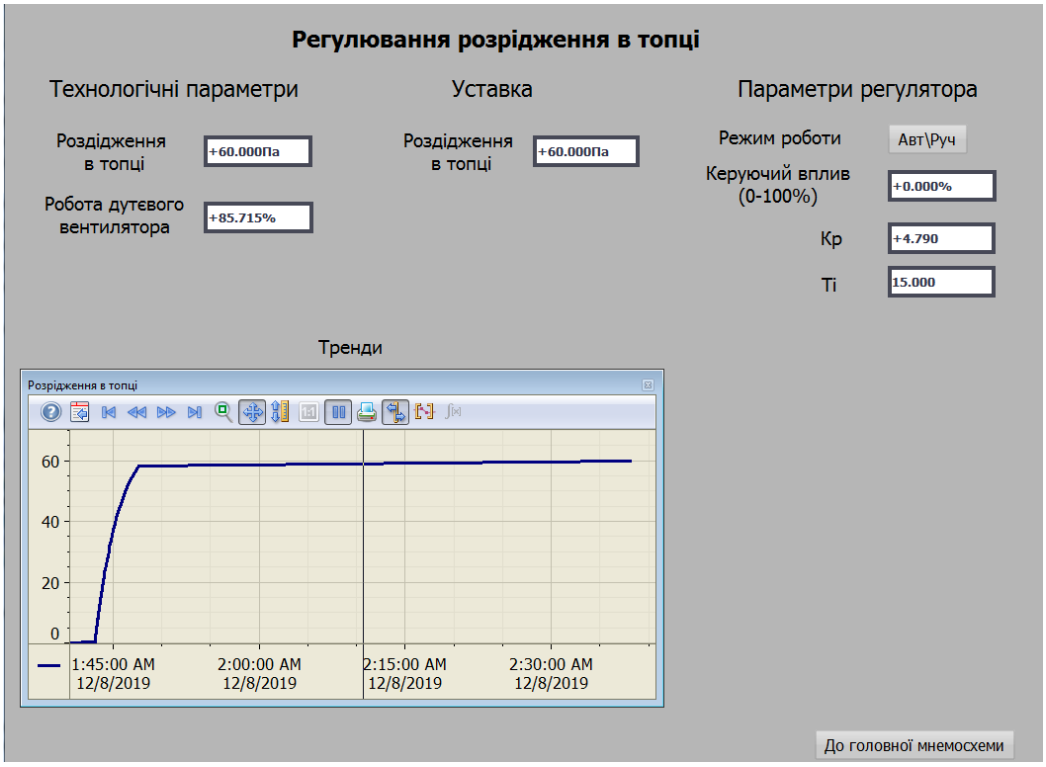


Рис. 3.22 Вікно регулювання розрідження в топці

ВИСНОВКИ ДО РОЗДІЛУ 3

У ході виконання даного розділу було розроблено програмне забезпечення супевізорного та локального рівняв ПТКЗА. Основою даної системи став контролер Siemens Simatic S7-300 з відповідними модулями вводу/виводу. WinCC Professional взяв на себе функції супервізорного рівня, так як на його платформі запускаються вікна візуалізації.

Супервізорний рівень забезпечує можливість ручного керування, моніторинг технологічних параметрів та можливість зміни уставки, регулюючого впливу. Також відображає аварії, які виникають та тренди регульованих технологічних параметрів.

4. ОРГАНІЗАЦІЯ КІБЕРБЕЗПЕКИ В ПІДСИСТЕМІ КЕРУВАННЯ ПРОЦЕСОМ ГОРІННЯ КОЛОАГРЕГАТУ НА ТВЕРДОМУ ПАЛИВІ

В сучасному світі все частіше зустрічаються факти порушення безпеки в системах АСУТП. Як наслідок, виникає потреба щоб обслуговуючий персонал, інженери мали необхідні знання для виявлення, класифікацію та зменшення наслідків від кібератаки.

Захищеність системи керування процесом горіння котлоагрегату визначається вдалим вирішенням таких питань:

• Які можливі шляхи для злому системи?

• Які вразливі системи існують і до яких наслідків це може призвести?

• Які максимальні збитки можуть бути заподіяні при втручанні в роботу системи?

• Які засоби безпеки впроваджені та захищають об'єкт управління?

• Хто відповідальний за заходи безпеки?

Для того, щоб підтримувати безпеку системи, потрібно спершу забезпечити безпечність самих операційних процесів і зв'язку між ними.[1]

4.1 ППРОЦЕДУРА ВІДНОВЛЕННЯ ПІСЛЯ КІБЕРАТАКИ

Простій роботи котла, який використовується для виготовлення напівфабрикату паркетної дошки може спричинити суттєві втрати в силу того, що час заміни обладнання може займати місяці і за весь цей період підприємство не буде отримувати дохід, а розхідна частина залишиться тією ж. Персонал повинен знати методи, використовуючи які хакери можуть напасти на промислове обладнання і пошкодити операційну інфраструктуру підприємства. На практиці це означає, що[1]:

• в існуючих на сьогодні протоколах для систем керування майже немає засобів безпеки;

• в промислових мережах використовується протокол TCP / IP з властивими йому вразливостями;

• високий попит на дистанційну керування та діагностику, що підвищує вразливість системи;

• взаємозв’язок промислової та корпоративної мереж більше підвищує вразливість;

• використання несучасних операційних систем та програмних засобів з несучасною організацією механізму оновлень приводить до збільшення можливостей для доступу хакерів до АСУ ТП;

• недостатність наявного моніторингу систем управління для виявлення вторгнення хакерів;

• не забезпечення захисту продуктів постачальниками;

• ПЛК встановлюються з ввімкненими веб-службами, та багато користувачів залишають веб-сервери ПЛК активними і не конфігурованими, з паролями за замовчуванням;

• значно підвищився інтерес до операційних систем керування з боку іноземних спецслужб і терористів;

• немає можливостей для автенифікації команд та виявлення шкідливого програмного забезпечення на застарілих ПЛК.

Великі компанії, такі як Tarkett, розміщують інформацію про підприємства в «хмарі», для лекшого менеджменту підприємств, не враховуючи те, що напад на один об'єкт може поширитися і на інші.

4.1.1 МЕТА ПРОЦЕДУР ВІДНОВЛЕННЯ

Мета процедури відновлення після кібератаки полягає в тому, щоб зупинити кібератаку та відновити важливі процеси.

■ **Програмне забезпечення веб-сервера**, вбудоване в пристрій системи керування, що надається для віддаленого налаштування системи керування з веб-браузера. Воно також дистанційно використовується постачальниками обладнання для оновлення програмного забезпечення або усунення неполадок.

Це важливий момент, тому що коли ви питаєте інженера з технічного обслуговування, чи можна відключити засоби контролю безпеки на котлі, щоб подача палива не припинялася автоматично у випадках коли полум'я гасне або коли подача води в котел зупинена, відповідь зазвичай: «Звичайно, але навіщо вам це потрібно?» Шаблон процедури відновлення повинен містити загальні

форми, які повинні бути налаштовані для конкретних елементів системи управління. Вони служать у якості центрального сховища для інформації, завдань і процедур, які необхідні будуть технічному персоналу для відновлення функцій критичного обладнання у разі виникнення інциденту.

Перш за все, коли виявлена кібер-фізична атака, рекомендовано фізично витягнути вилку живлення комп'ютера з розетки, а не завершувати роботу системи стандартним чином. Поточні дані (і не тільки) в системі можуть бути повністю знищені, якщо операційна система виконує звичайний процес зупинки. Крім того, потрібно уникати запуску будь-якого антивірусного програмного забезпечення «після факту», оскільки антивірусне сканування змінює критичні дати файлів і перешкоджає виявленню та аналізу підозрілих шкідливих файлів. По-друге, добре спроектована і скоординована кібер-фізична атака буде включати кібер-пастки, призначені для того, щоб продовжувати завдавати шкоди, коли обслуговуючий персонал намагається відновити нормальну роботу обладнання.

■ **Кібер-пастка**. Хакер впроваджує шкідливе ПЗ, що повинно викликати катастрофічні дії персоналу з обслуговування котла. Наприклад, початкова індикація кібер-атаки може полягати в тому, що хакер вимкнув подачу води в котел. Технічний персонал в диспетчерській не знає, що шкідлива програма до того викачала всю воду з котла і підвищує температуру в ньому. Як тільки котел перегріється, наступна подача води викличе вибух. Хакеру необхідно ініціювати саме таку дію обслуговуючого персоналу, щоб збільшити збиток.

Кібернетичні пастки - "скрипти" (подібні до макросу), закладені хакером, які несвідомо ініціюються діями персоналу служби технічного обслуговування, такими як перемикання чого-небудь, увімкнення або вимкнення прихованого зловмисного програмного забезпечення. Хакер розраховує дії поводження обслуговуючого персоналу таким чином, щоб кібер-фізична атака продовжувала тривати і після втрати доступу хакера до вразливостей системи. Якщо поставити процедури відновлення на сервер, який був зламаний, точна послідовність дій

персоналу, що обслуговує ці операції, може бути заздалегідь відома хакерам. Хакер буде використовувати процедури відновлення проти нас.

За такого передбачення на руках хакера - "інженера" існує конкретний сценарій кібер-фізичної атаки об'єкта, і він залежить від тригерів, які він передбачив, щоб продовжувати атаку. Без цих тригерів кібер-фізична атака може бути зупинена. Для того щоб зупинити дану атаку не потрібно витрачати час на виявлення тригерів (це можна буде зробити пізніше), а треба просто вимкнути сервера АСУ ТП і повернутись до повного ручного управління, таким чином зірвавши скриптову кібер-пастку.

Важливо розуміти, що метою хакерів є серйозні пошкодження критичних систем, а використовувані шкідливі програми дуже складні. Просте повернення живлення обладнання після відключення АСУ від Інтернету не означає, кібер-атака завершена. Шкідливе ПЗ вже знаходиться у системі керування і атака може продовжитись навіть після виправлення вразливостей системи. Конструкції кібер-пасток варіюються в залежності від механізму тригера, корисної завантаженості та величини шкоди, яку хакер має намір викликати.

Кібер-пастка може реагувати з нульовою затримкою, або вона може бути запрограмована з якоюсь часовою затримкою, щоб заплутати технічний персонал. Майстерність розміщення кібер-пастки полягає в використанні природної поведінки людей (тобто, знання соціальної психології), такої як звичка, цікавість або допитливість, або в розумінні стандартних дій обслуговуючого персонала, що на перший погляд виглядають простим вирішенням складної проблеми.

Майже будь-яка частина програмованого обладнання може мати якусь кібер-пастку. Єдиними обмеженнями до складності кібер-пасток є майстерність та винахідливість хакерів, які їх розміщують. Наприклад, підробка значення тиску всередині котла, може бути використана як «наживка». Натомість, спроба перезапуску котла може активувати інші приховані кібер-пастки, призначені для пошкодження пристроїв подачі повітря, ввімкнення освітлення або видачу помилкових пожежних сигналів. Кібер-пастки закладають до системи в будь-

якій ситуації, коли існує сильна імовірність того, що вони запустяться обслуговуючим персоналом, особливо в критичних ситуаціях. Щоб заподіяти найбільшу шкоду критичним одиницям обладнання, хакер встановить багато кібер-пасток, кожна з яких ініціює певний набір "небажаних подій". Що у свою чергу призведе до виникнення декількох атак одночасно.

Коли спрацьовує кібер-пастка, це може спричинити перехід обладнання в режим "аварія". Далі можливо вмикання чи вимикання обладнання, зміна параметрів встановлених завдань, зміна числа обертів двигуна, збільшення або зменшення тиску рідини або якого-небудь іншого значення та інші дії. Вона може призвести до того, що дисплеї комп'ютера залишаться порожніми або будуть відображати неправильну інформацію про роботу обладнання. Обладнання може працювати неефективно; програмне забезпечення може бути модифіковане таким чином, що оператор вводить команду, щоб зменшити тиск води, а фактично збільшує її тиск. Або, спроба затримки одного аларма викликає інший аларм[1].

■ **Canary** (канарка)– це будь-що, що може відправити сповіщення, якщо щось трапиться у системі. Якщо все ж щось стається, ви знаєте, що це за межами нормальної поведінки[1].

Вони використовуються для попередження персоналу, коли помічена невластива поведінка системи(коли хакери ще ховаються у тіні).

■ **Honeypot** ("медова" пастка). Система (наприклад, веб-сервер) або системний ресурс (наприклад, файл на сервері), який розроблений таким чином, щоб бути привабливим для потенційних зловмисників та порушників, і не має жодних авторизованих користувачів, крім адміністраторів. (Джерело: CNSSI-4009). Вона дозволяє перемкнути увагу зловмисника з атаки критично важливого обладнання на щось неважливе, що контролюється автоматичною системою попередження вторгнення[1].

Процедури відновлення призначені для реалізації планів забезпечення безпеки працівників та відновлення з часом роботи обладнання. Незважаючи на те, що в процедурі відновлення наводяться керівні вказівки та документація, на

основі яких здійснюються заходи у надзвичайних ситуаціях, саме по собі відновлення та планування відновлення не призначене як заміна для обґрунтованого прийняття рішень. Індивідуальні процедури відновлення повинні містити детальні дії персоналу та конкретні завдання для заходів з реагування на надзвичайні ситуації та операції по відновленню роботи об’єкта на основі заздалегідь визначених часових термінів. Документ про процедури відновлення не є одноразовим зобов'язанням із фіксованою датою початку та закінчення. Це постійна, належним чином профінансована охоронна діяльність, спрямована на забезпечення необхідних ресурсів для:

• виконання заходів, необхідних для побудови планів відновлення та самого відновлення;

• кваліфікаційної підготовки та перепідготовки працівників;

• розробки та перегляду політик та стандартів у процесі еволюції кібер-загроз;

• повторної реалізації вже досягнутих цілей;

• постійного сповіщення керівництва;

• процесу дослідження змін та технології для підвищення ефективності відновлення;

• виконання плану технічного обслуговування.

Розробка процедур відновлення, що включає в себе заходи, необхідні для підтримки життєздатної безперервності, потребує послідовної методології планування. Елементи процедури відновлення, необхідні для створення життєздатних, повторюваних і перевірених можливостей включають до себе:

• впровадження точних та неперервних життєво важливих заходів, резервного копіювання даних та зберігання копій поза місцем їх використання;

• впровадження можливостей для швидкого відключення комунікаційних каналів;

• забезпечення альтернативного ручного керування роботою обладнання;

• створення групи реагування на інцидент;

• реалізації стратегій непередбачуваних випадків.

■ **Розклад кібер-атак**. Це графік хакерів під час підготовки до кібер-атаки. Вона починається з розвідки цілі. Супротивник вирішує націлитись на об'єкт та досліджує середовище майбутньої атаки, шукає вразливості. Веб-додатки з відкритим кодом на корпоративному веб-сайті, постачальники, а також списки учасників різноманітних онлайн-конференцій дають зловмиснику якомога більше інформації про технічний персонал. Супротивник відстежує мережу керування і формує стратегію нападу, використовуючи інформацію про організацію, об'єкти і персонал за допомогою відкритого коду. Як тільки противник має стратегію нападу, він почне озброюватися відповідним набором інструментів нападу та розробляти програмний пакет для доставки та виконання шкідливого коду у мережі керування. Супротивник створює сховище інструментів кібер-фізичної атаки, які використовують декілька вразливих місць у системі захисту з нульовим часом, спеціально розроблених для того, щоб завдати значних збитків і забезпечити декілька місяців ремонту.

Коли противник отримує зелене світло для атаки, він уже готовий розпочати атаку кожної миті. Можливо, він вже встановив інструменти нападу (зловмисне програмне забезпечення) у системі без відома, незважаючи на те, що це не легко приховати.

Коли настає повномасштабна кібер-фізична атака, супротивник розробить її таким чином, щоб її наслідки міг ще погіршити своїми діями ваш персонал при її ліквідації. Атака розробляється таким чином, щоб персонал, завдав при її ліквідації ще більше шкоди обладнанню, розповсюдив атаку на інші об'єкти та, можливо, створив ще більше вразливостей у ПЗ.

4.1.2 ІНФОРМАЦІЯ ПРО ПРОЦЕДУРИ ВІДНОВЛЕННЯ

Процедура відновлення має містити інформацію, яка залишається постійною та інформацію, яку потрібно регулярно оновлювати. Статична інформація повинна бути визначеною та зрозумілою усім працівникам.

Застосовні директиви

Керівництво повинно підтримувати інфраструктуру забезпечення інформаційної безпеки, яка гарантує, що її інформаційні ресурси підтримують

доступність, конфіденційність, цілісність та не відмову від своїх даних. Крім того, менеджмент повинен захистити свої стратегічні можливості управління інформаційними ресурсами. Тому ця процедура відновлення Cyber-Physical Attack була розроблена відповідно до наступних виконавчих рішень, нормативних повноважень, положень та директив:

• Закон України «Про основні засади забезпечення кібербезпеки України» Відомості Верховної Ради, 2017, №45, ст.403.

• «Рекомендації щодо створення надійних автоматизованих систем керування технологічними процесами» розроблені Національним інститутом стандартів та технологій США 800-82[3].

Цілі плану Організації залежать від різних IT-систем, класифікованих як загальна система підтримки (GSS), які забезпечують критично важливі функції зв'язку, доступу до Інтернету та електронної пошти або основних додатків (MA). Незважаючи на те, що багато загроз та вразливостей можна пом'якшити, деяким з загроз не можна запобігти. Тому важливо, щоб в експлуатуючій організації були розроблені процедури відновлення для забезпечення безперервного виконання усіх функцій системи автоматизації.

Основний акцент у процедурі відновлення полягає в захисті двох важливих активів будь-якої організації: персоналу та обладнання. Всі аспекти процедур відновлення повинні бути спрямовані на захист та безпеку персоналу, а також на захист та відновлення обладнання до повного функціонування. Це включає в себе встановлення оперативної спроможності обробляти попередньо визначені критичні додатки, відновлення даних з наборів резервних копій поза об'єктами та відновлення уражених систем до нормального робочого стану. Процедури відновлення спрямовані на виконання наступних додаткових завдань:

• мінімізувати кількість рішень, які повинні бути прийняті під час кібер-фізичної атаки;

• визначити ресурси, необхідні для виконання дій, визначених цим планом;

• визначення дій, які мають бути виконані заздалегідь призначеними командами спеціалістів підприємства;

• визначення критичних даних системи автоматизації у поєднанні з клієнтами, які будуть відновлені під час періоду відновлення операцій;

• визначення процесів для тестування та ведення процедур та тренінгів персоналу з непередбачених обставин.

4.2 КОМАНДИ ЩО РЕАГУЮТЬ НА КАТАСТРОФИ

У разі кібер-фізичної атаки нормальна робота організації зміниться непередбачувано. Основна увага системи управління котлом переміститься від існуючої структури та функцій «звичайної роботи» до структури та функціонування системи управління, яка прагне до відновлення операцій. У цій процедурі відновлення співробітники служби підтримки котельної установки, співробітники IT та персонал з питань безпеки працюватимуть у групах реагування на катастрофи (IRT) на етапах виявлення, пом'якшення наслідків та відновлення. Кожен етап вимагає, щоб команди, що виконують ці процедури, тісно співпрацювали.

Кожна з команд повинна складатися з осіб з особливими обов'язками, які повинні бути заздалегідь визначені, щоб повністю виконати план. Буде щонайменше чотири команди: команда з керування відновленням, команда з технічного обслуговування, команда з питань безпеки та команда технічної підтримки. Основні та альтернативні очільники команд вказуються під час підготовки документів щодо процедур відновлення. Метою кожної команди є відновлення та повернення до стабільних та нормальних операцій. Кожен керівник команди повідомляє про статус відновлення та його оновлення в Координаційний центр підприємства.

Головні обов'язки команди по відновленню після інцидента:

• захистити працівників та обладнання, доки не буде відновлена звичайна робота технологічного обладнання;

• забезпечити спроможність реакції на атаку;

• управління реагуванням та відновленням діяльності;

• підтримка та спілкування з працівниками, системними адміністраторами, працівниками служби безпеки та керівниками;

• швидке та ефективне відновлення операцій, технологій;

• забезпечити виконання нормативних вимог законодавства;

• виконувати рішення щодо відновлення операційної діяльності та відшкодування витрат підприємства.

4.2.1 КОМАНДА З КЕРУВАННЯМ ВІДНОВЛЕННЯМ(MGMT)

Команду з керування відновленням після інциденту очолює Координатор процедур відновлення, який відповідає за адміністративні, логістичні та громадські відносини у процесі відновлення. Керівники інших команд повідомляють цю команду під час кібер-фізичної атаки. Кожна з цих команд очолюється одним із членів MGMT.

MGMT несе відповідальність за наступне:

• оцінка шкоди та, за необхідності, оголошення про напад (форми оцінки пошкоджень попередньо повинні бути включені до відповідного плану);

• координація зусиль усіх інших команд;

• затвердження всіх дій, які не були заплановані;

• стратегічне керівництво;

• за зв'язок з вищим керівництвом;

• прискорення вирішення поточних питань, уникаючи всі бюрократичні процедури;

• надання консультації тим працівникам, які запитують або вимагають цього.

4.2.1.1 ВИКОНУВАННІ КОМАНДОЮ ПРОЦЕДУРИ ЗА ЕТАПАМИ

MGMT виконує наступні завдання на таких етапах:

Етап 1: Виявлення

• активізує групи реагування на інциденти ;

• виконує швидкі перевірки систем ;

• оголошує про кібератаку і повідомляє адміністрацію верхнього рівня;

• вирішує, чи залишається об’єкт безпечним, чи потрібно евакуювати працівників.

Етап 2: Пом'якшення наслідків

• створює командний центр;

• при необхідності, евакуює працівників об’єкту;

• робить пріоритетною роботу з відновлення функціонування операційних технологій;

• координує діяльність інших груп реагування на інциденти.

Фаза 3: Відновлення

• координує діяльність інших груп з реагування на інциденти ;

• займається відновленням об’єкту та відновленням звичайних операцій;

• інформувати керівництво.

4.2.2 КОМАНДА З ТЕХНІЧНОГО ОБСЛУГОВУВАННЯ(FAC)

Команда з технічного обслуговування відповідає за мінімізацію збитків від пошкодження обладнання на початковому етапі. Також швидко визначає, яке обладнання можна відновити, а яке ні. Виконує замовлення на ремонт та заміну обладнання, яке знаходиться не в робочому стані. FAC відповідає за розміщення необхідного нового обладнання та нагляд за заміною старого обладнання та впровадженням нового.

4.2.2.1 ВИКОНУВАННІ КОМАНДОЮ ПРОЦЕДУРИ ЗА ЕТАПАМИ

FAC виконує наступні завдання на таких етапах:

Етап 1: Виявлення

• мобілізація команди технічного обслуговування;

• перевірка пристроїв.

Етап 2: Пом'якшення наслідків

• оцінка пошкоджень;

• визначення вимог до заміни обладнання;

• інвентаризація всього устаткування.

При необхідності залучаються постачальники обладнання.

Етап 3: Відновлення

• збереження обладнання та витратних матеріалів;

• замовлення нового технологічного та комп'ютерного обладнання;

• організує встановлення та тестування нового обладнання;

• співпрацює з підрядниками та персоналом для відновлення операцій;

• контролює встановлення нового обладнання.

4.2.3 КОМАНДА ТЕХНІЧНОЇ ПІДТРИМКИ (TECH)

Команда технічної підтримки відповідає за експлуатацію та обслуговування АСУ ТП. Відповідальність команди TECH поширюється на конфігурування та встановлення серверів та робочих станцій. Команда TECH повинна відновити та переналагодити програмне забезпечення на первинному рівні. Крім того, команда TECH надає технічну підтримку іншим командам.

4.2.3.1 ВИКОНУВАННІ КОМАНДОЮ ПРОЦЕДУРИ ЗА ЕТАПАМИ

TECH виконує наступні завдання на таких етапах:

Фаза 1: Виявлення

• мобілізація команди технічної підтримки;

• початок перевірок системи управління.

Фаза 2: Пом'якшення.

• тестування обладнання та програмного забезпечення;

• визначення обсягу пошкоджень для серверів і робочих станцій;

• робота з відповідними постачальниками.

Фаза 3: Відновлення

• замовлення потрібного обладнання та матеріалів;

• відновлення серверів і робочих станцій;

• встановлення та налаштування додатків та ОС;

• тестування обладнання та програмного забезпечення;

• співпраця з відповідними постачальниками для отримання допомоги у відновленні;

• перевірка того, що системи після відновлення працюють так як повинні.

4.2.4 КОМАНДА БЕЗПЕКИ ВІДНОВЛЕННЯ (SEC)

Відповідальність команди SEC включає до себе операції фізичної безпеки та збирання, транспортування всіх IT-серверів та результатів недавнього

резервного копіювання даних для судової експертизи. Ця команда також несе відповідальність за забезпечення безпеки об’єкту на час інциденту.

4.2.4.1 ПРОЦЕДУРИ ЗА ЕТАПАМИ

Група безпеки виконує наступні завдання на наступних етапах:

Етап 1: Виявлення

• мобілізація команди з безпеки;

• початок швидких перевірок системи управління.

Етап 2: Пом'якшення

• інвентаризація та захист резервних копій;

• транспортування серверів та даних (атаки) для виконання процедур цифрової криміналістики.

Етап 3: Відновлення

• забезпечення фізичної безпеки в будівлі;

• допомога всім командам у відновленні виробничого середовища;

• забезпечення супроводу працівників;

• сприяння відновленню системи безпеки та відеоспостереження до стану нормальної роботи;

• моніторинг об’єкта з ціллю виявлення незвичної аномальної поведінки;

• моніторинг поставок;

• надання послуг супроводження для перевізників.

4.3 ВИЯВЛЕННЯ КІБЕРАТАК СПРЯМОВАНИХ НА ФІЗИЧНЕ ПОШКОДЖЕННЯ КОТЛА

Мережа АСУ не має бути доступна зовні організації. Але, якщо існує потреба мати дистанційний доступ та підключення, то якщо існують такі фактори атаки як збільшення частоти сканування портів або різке зростання кількості спроб, як запобіжний захід всі зовнішні з'єднання мають бути розірвані.

Першою ознакою того, що кібератака ведеться, можуть бути сигнали від АСУТП, які вказують на те, що у певному обладнанні сталася поломка/аварія. Складна атака використовує декілька вразливостей щоб антивірусні системи не виявляли їх. Автоматичне виявлення кібератаки за допомогою програмових

засобів таких як: аналізатори мережевого трафіку , мережеві монітори, IDS, які можуть виявити шкідливі програми, спроби злому, порушення політик.

Обслуговуючий персонал, технологи дізнаються про атаку швидше, ніж IT персонал або системні адміністратори, бо вони безпосередньо бачать зміну роботи обладнання. Досвідчений персонал є найкращим детектором для виявлення ненормальної поведінки..

Індикатор - визначена дія (конкретна, узагальнена, або теоретична), яку зловмисник може вчинити в ході підготовки до нападу. (Джерело: CNSSI-4009)

Нижче приведено індикатори, які треба розглядати як показники початку кібератаки[1]:

1. Незвично великий мережевий трафік
2. Зменшення місця на диску або дефіцит на серверах
3. Незвично висока продуктивність процесора
4. Створення нових облікових записів користувачів
5. Використання облікових записів рівня адміністратора
6. Заблоковані облікові записи
7. Облікові записи використовуються, коли користувач не на роботі
8. Очищені файли журналів
9. Повні лог-файли з великою кількістю подій
10. IDS оповіщення
11. Несподівані зміни патчів
12. Підключення обладнання за зовнішніми IP-адресами
13. Запити на отримання інформації про систему
14. Несподівані зміни параметрів конфігурації
15. Несподіване завершення роботи системи
16. Зупинка або відображення повідомлень про помилки у веб-базах даних або сервері з прикладними програмами
17. Незвично повільний доступ до вузлів мережі

18. Імена файлів, що містять незвичайні символи або нові чи несподівані файли і каталоги

19. Велика кількість заблокованих електронних листів з підозрілим вмістом

20. Незвичайне відхилення від типового розподілу мережевих транспортних потоків

21. Нестабільна поведінка обладнання, особливо, коли більш ніж один пристрій має таку нестійку поведінку

22. Будь-яке очевидне перевизначення параметрів безпеки, резервного копіювання або відмово-стійкості систем.

23. Обладнання, сервера або мережевий трафік, який має сплески тимчасового високого використання, коли сам поточний процес є стійким і передбачуваним.

24. Невідомий трафік з корпоративної або іншої мережі

25. Невідоме завантаження/вивантаження мікропрограм

Система виявлення вторгнень, яка застосовується на підпримстві NFR IDS, призначена для виявлення цільових/нецільових подій.

4.3.1 УПРАВЛІННЯ ПОЗАШТАТНИМИ СИТУАЦІЯМИ

Деколи, вихід з ладу частини обладнання може привести до виходу з ладу іншого обладнання. Фільтрація сигналу тривоги, дає можливість визначити початкову помилку та встановити їй більший пріорітет, таким чином визначаючи обладнання, яке потрібно відремонтувати в першу чергу.

Добре спланована атака представляє собою динамічний процес, а швидкість реакції визначає ступінь наслідків. Дослідження ASM показали, що затримка в повній обробці сигналу тривоги для кваліфікованого фахівця становить 10 хвилин (див. рис. 4.1)

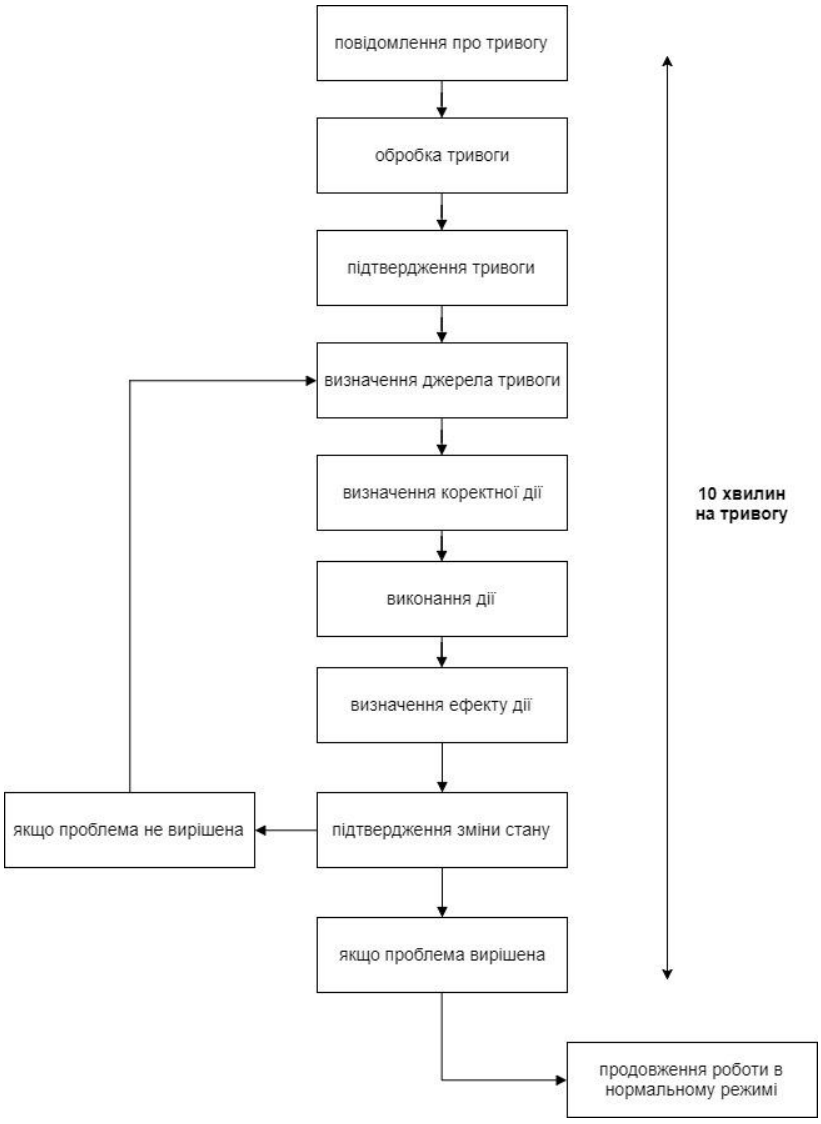


Рис.4.1 Обробка сигналу тривоги

Детектування події - це лише початковий етап, IDS має подати дані в зручному для оператора форматі.

4.4 ІНСТРУМЕНТИ РЕАГУВАННЯ НА АТАКУ

Інструменти, що використовуються для виявлення потенційної кібератаки під час рутинних операцій:

- Програма для аналізу мережевих пакетів Wireshark забезпечує:
  - *Збір і аналіз трафіку мережі.* Дозволяє бачити все що відбувається у мережі, та ізолювати дані домену промислової мережі. Також зберігати дані як для подальшого аналізу і для судової експертизи.

- *Реконструктор пакетів і трафіку.* Допоможе повернути файли до початкового формату, врезультаті фіксуючи статичний образ мережі та пов'язаний з ним трафік.
- *Аналізатор протоколу.* Зберігає та фіксує інформацію про пакет, та включає статистичну інформацію для подальшого використання методів цифрової криміналістики.

- Програмне забезпечення SolarWinds Server & Application Monitor забезпечує:
  - *Моніторинг продуктивності мережі.* Завдяки ньому системні адміністратори можуть визначити, де відбувається незвично висока активність.
  - *Контроль програмових засобів.* Відстеження роботи певних програм, якщо існує підозра на маніпулювання або несанкціонований доступ, та дозволяє зробити більш ретельний аналіз програми в порівнянні з загальним моніторингом мережі.

4.4 КАТЕГОРИЗАЦІЯ АТАК

Після того, як ідентифіковано атаку, вона повинна бути класифікована, і прийнята відповідна реакція на неї (табл.4.1) та пріоритет виконання на основі цієї категоризації[1]. Активність відновлення матиме пріоритет (див табл. 4.1)

Таблиця 4.1 Точки прийняття рішень при атаці та відповідні дії

Точка прийняття рішенння	Дії				Категорія
1. Кібер подія виявляется IDS; або ж є непередбачений збій в роботі обладнання	2. Подія підтверджується як кібератака	3.Запускається процедура відновлення	4.Звучить тривога	5. Котельню евакуюють	Ініціація
	2. Якщо ні, то	3.Не запускається процедура відновлення	4. Повернення до нормальних операцій	5. Оцінка реакції	Визначення
6. Визначення обсягу атаки та оцінка втрат	7. Якщо втрат майже немає, то	8. Відновлення та очистка	9. Повернення до нормальних операцій	10. Повідомити менеджмент про ситуацію	Коротка евакуація може знадобитись
	7. Середні та великі втрати	8.Переміщення на нове місце	9. Виклик команди відновлення	10. Повідомити менеджмент про ситуацію	Середній чи високий рівень ушкоджень

Продовження таблиці 4.1

11. Оцінка пошкоджень	12. Якщо пошкодження можна відновити менш ніж за 30 днів	13. Виконати роботу з відновлення	14. Повернення персоналу на об’єкт	15. Повернення до нормальної роботи	Середній рівень ушкоджень
	12. Якщо пошкодження можна відновити більш ніж за 30 днів	13. Замовити поставки та устаткування	14. Тимчасове припинення роботи котла поки іде ремонт	15. Повернення до нормальної роботи	Високий рівень ушкоджень
	12. Якщо не можна відновити	13. Перебудувати	14. Призупинення роботи котельні	15. Повернення до нормальної роботи	

4.5 ПОМ’ЯКШЕННЯ НАСЛІДКІВ

Змншення наслідків і відокремлення частин необхідне, щоб запобігти поширенню шкідливих програм на ще не заражені сегменти системи і технологічне обладнання. Хакер може залишити багато шкідливих програм в АСУ, у тому числі шкідливі програми, які він встановив першими - зворотній виклик процедури, яка автоматично намагається підключитися до сервера атаки, якщо система була відключена або перезавантажена. При наявності процедури пом’якшення наслідків, у хакера зникне можливість робити подальші пошкодження системи; вона наддасть час обслуговуючому персоналу уважно вивчити котел та обладнання, виконати перезапуск обладнання вручну,

виконати заміну всіх серверів і подальше відновлення АСУ ТП до нормального стану.

Після того, як встановлено, що почалася кібератака, потрібно переводити роботу технологічного устаткування на ручне керування і покладатися на уміння персоналу використовувати свої знання та навики при швидкій зміні ситуації. Тимчасова зупинка автоматичних служб і перехід на ручне керування обладнанням є потенційно руйнівною мірою, але це найбільш безпечний шлях. Систему керування котлоагрегатом було розроблено таким чином, що оператор з легкістю може переключити керування з автоматичного в ручний режим роботи. Це дозволяє зменшити вплив кібератаки з найменшою вратою функціональності, перевівши котел в ручне керування.

4.6 ВИРІШЕННЯ ПРОБЛЕМ

У разі кібератаки проти обладнання або систем, симптомами проблеми може бути багато можливих причин. Проблема спочатку проявляється у вигляді якихось несправностей. Будь-яка несподівана або небажана поведінка системи керування є можливою ознакою атаки. Проста заміна зламаної частини обладнання, такої як насос або двигун, буде марною без ліквідації джерела проблеми – «хакнутої» АСУ.

Багато АСУ можуть генерувати звіти для усунення неполадок. Якщо проблема помічена, то важливо зразу дивитися на всі початкові налаштування і будь-які можливі подальші перевизначення параметрів, щоб визначитися з причиною.

4.6.1 КРОКИ ВИРІШЕННЯ ПРОБЛЕМ

КРОК 1. Впевнитися в тому, що подія є кібератакою

КРОК 2. Сповільнити атаку, вважаючи, що АСУ вже не під контролем

КРОК 3. Зупинити атаку.

КРОК 4. Оцінити пошкодження у всьому несправному обладнані, вважаючи що все обладнання було «хакнуте»

КРОК 5. Відновити програмне забезпечення на заражених серверах та відновити пошкоджене обладнання

КРОК 6. Перезавантажити АСУ та перезапустити автоматичну роботу/операції

4.7 ЗАПОБІГАННЯ ВПЛИВУ ХАКЕРІВ НА СИСТЕМИ КОТЛА

Котел є закритим об’єктом під тиском, в якому вода або інша рідина використовується для обігріву будівлі та сушки деревини. Хакер може використати декілька векторів атак для виводу його з нормального режиму роботи, часткового блокування, або повного вимкнення. Наприклад, переривання подачі палива в топку котла заважатиме процесу згоряння і може призвести до зупинки роботи котла. При подальшому запуску, якщо вода попаде в порожній розігрітий котел, вона миттєво закипає при контакті з перегрітою металевою оболонкою і призводить до сильного вибуху пари, що не зможе контролюватися навіть при наявності запобіжних клапанів.

Технологічні параметри АСУ котла, на котрі може бути звернена увага зловмисника і які повинні захищатися:

- Температура води, що подається
- Температура димових газів
- Витрата палива
- Сигнал полум'я
- Ефективність горіння
- Значення O2
- Тиск в котлі
- Витрата первинного і вторинного повітря
- Історія несправностей

4.7.1 ОСОБЛИВОСТІ ЗАХИСТУ КОТЛА ВІД ПОШКОДЖЕННЯ

4.7.1.1 ВИБУХ КОТЛА

Вважається, що це не може відбутися через систему безпеки, призначену для запобігання катастрофі. Але хакер вимкне функції безпеки без

відома. Неможливість захистити котел від кібератаки може (і швидше за все) призведе до катастрофи. Найпоширеніші способи "знищити котел" кібератакою наведені нижче:

- *Вибух палива*
- *Неправильний розігрів*
- *Неправильний рівень тиску у котлі*
- *Згасання полум'я*
- *Надмірне полум'я*

Найбільш небезпечною ситуацією є вибух палива в котлі. Умови для вибуху можуть бути викликані діями хакера, який зловмисно змінює профіль конфігурації (робочі параметри) системи, тому АСУТП продовжує "думати", що котел працює належним чином, коли насправді поточний стан вже вийшов за межі виробничіх налаштувань. Сигналу тривоги при цьому не буде по причині того, що хакер його відключив. Викликати вибух котла можливо, наприклад, в такий спосіб:

• *Подати до топки багато паливної суміші* : хакер може використовувати АСУТП для створення високих концентрацій незгорілого палива, через недостатність повітря для палива, що спалюється. Хакер при цьому, розраховує на подальші дії обслуговуючого персоналу, який стане додавати повітря до топки в агрегаті, що і призведе до подальшого вибуху.

• *Погана атомізація палива* : накопичення будь-якого незгорілого горючого палива може призвести до вибуху. Хакер збільшує тиск пари повітря і збільшує тиск палива набагато вище робочих налаштувань виробника.

4.7.1.2 ВИБУХ ГАРЯЧОГО ВОДОНАГРІВАЧА

Гарячий водонагрівач знаходиться під великим тиском водяної пари.Тому його вибух буде мати величезну силу. Обладнання декількох найближчих кімнат та сушок деревини від точки вибуху можуть зруйнуватись, а люди в кімнаті бути поранені або вбиті. Важливо пам'ятати, що вибухова хвиля із котельної найшвидше розповсюджується по трубах.

4.7.2 ПРОФІЛАКТИЧНІ ЗАХОДИ

Наступні заходи повинні бути дотримані, щоб перешкодити хакерам зруйнувати котел:

• Слід ретельно перевірити причину помилки, перш ніж намагатися запалити котел знову.

• Періодично вести спостереження за полум'ям, щоб своєчасно виявити проблеми згоряння.

• Перед розпалюванням котла, завжди треба продувати піч повністю, щоб видути незгорілі гази. Це особливо важливо, якщо попередньо були витоки.

• Переконатися, що система очищення води працює належним чином.

• Ніколи не відключати індикатори низького рівня води.

• Ніколи не продувати стінки в той час, як котел працює.

• Крива розігріву котла повинна бути строго дотримана.

4.8 РОЗШАРУВАННЯ МЕРЕЖІ РОЗПОДІЛЕНОЇ СИСТЕМИ КЕРУВАННЯ КОТЛОАГРЕГАТОМ

4.8.1 СЕГМЕНТАЦІЯ ТА РОЗШАРУВАННЯ МЕРЕЖІ

На підприємстві «Таркетт-Вінісін» де заходиться наша АСК на даний момент не застосовується розшарування та сегментація мережевого трафіку, що створює серйозну загрозу кібератаки на АСК ТП. Метою даного розділу є пошук шляхів для мінімізації доступу до конференційної інформації.

Перш за все, потрібно відокремити корпоративну та промислову мережі, так як характер мережевого трафіку відрізняється один від одного, для корпоративної мережі важливим та навіть критичним є доступ до Інтернету, електронної пошти, віддалений доступ. В той же час для промислової мережі цей вид трафіку становить загрозу, існують суворі процедури зміни мережевого обладнання, конфігурації та заміни програмного забезпечення, що не вимагається для корпоративної мережі.

Зазвичай розшарування та сегментація мережі відбувається на шлюзі між доменами, масштабні АСК ТП мають декілька доменів, це зумовлено тим що у

великих системах керування часто існують операції які є більш критичними за інші і потребують більшого ступеня захисту, в цьому випадку застосовується сегментація мережі АСК ТП на підмережі. В даній роботі розглядається система, яка керується одним органом керування, контролером Siemens S7-300, тож сегментування мережі АСК ТП на підмережі не застосовується.

Для логічного розділення мережі на об’єкті застосовується шифрована приватна мережа VPN, а саме OpenVPN, вона використовуючи механізми шифрування розділяє мережевий трафік, а також блокує доступ до конференційної інформації не авторизованим користувачам та має двофакторну аутентифікацію.

4.8.2 ПРИСТРОЇ ЗАХИСТУ МЕЖ ДОМЕНІВ

До пристроїв захисту меж доменів належать брандмауери, маршрутизатори, шлюзи, системи для виявлення вторгнень, керовані інтерфейси та інші. Їхнім завданням є керування передачею інформації.

Для цілковитого обмеження обміну трафіком між промисловою та корпоративною мережею ми будемо використовувати демілітаризовану дону(DMZ), яка знаходитися між доменами безпеки, таким чином мережевий трафік з промислової мережі до корпоративної буде проходити через DMZ, яка підключена до брандмауера.

4.8.3 АРХІТЕКТУРА РОЗШАРУВАННЯ МЕРЕЖІ

На рис.2 представлена архітектура розшарування мережі керування котлоагрегатом. Використання демілітаризованої зони у поєднання з брандмауером значно посилює кібербезпеку підприємства. Демілітаризована зона по суті являє собою проміжну мережу в якій знаходиться сервіс архівування, доступ до якого необхідний як з промислової так і з корпоративної мережі[2].

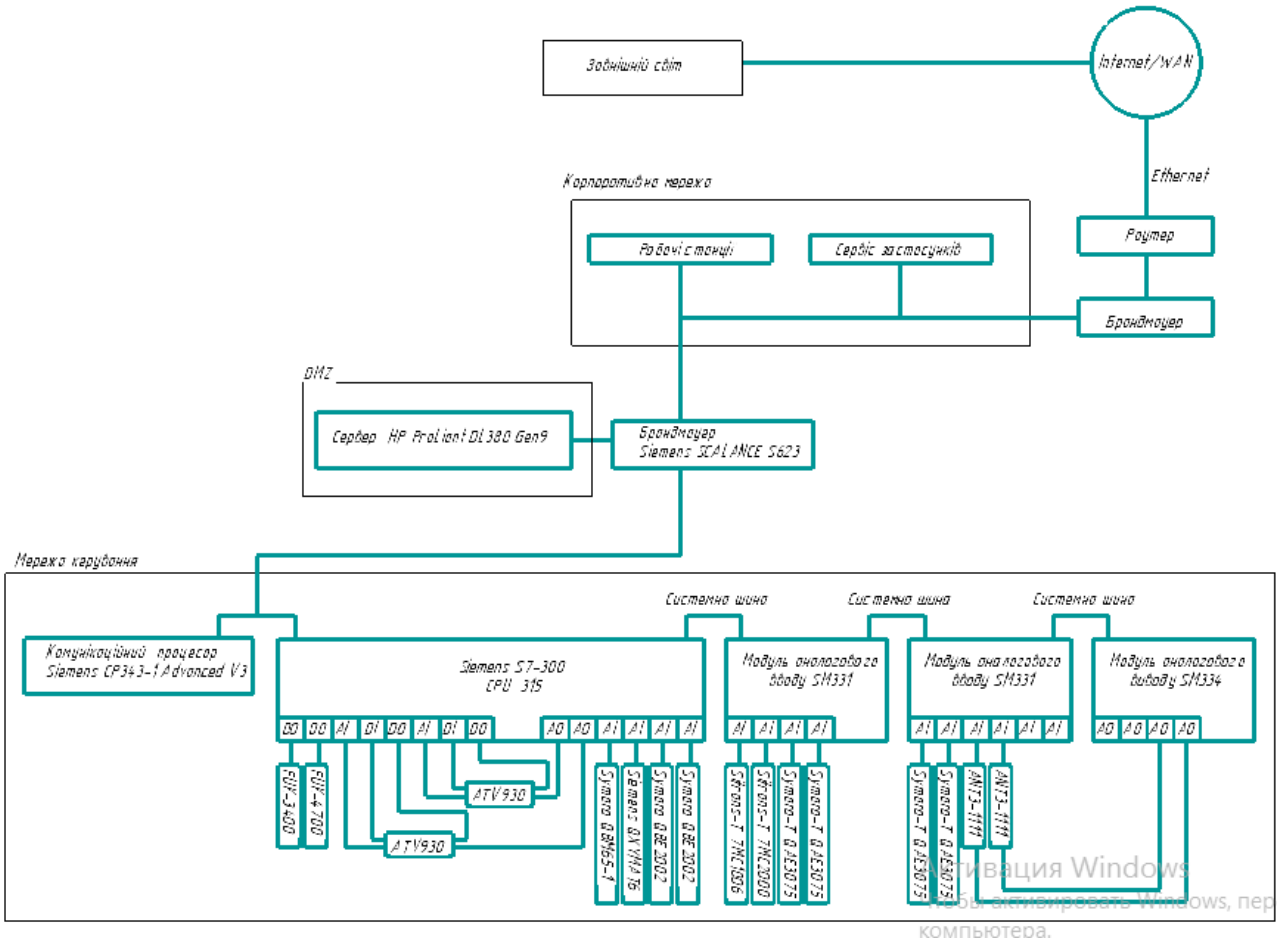


Рис. 4.2 Схема реалізації інформаційної безпеки котла КВм-1.75 за допомогою застосування брандмауера та демілітаризованої дони між корпоративною та промисловою мережами

В якості промислового брандмауера обрано Siemens SCALANCE S623, він має три мережеві порти, завдяки яким ми можемо налаштувати нашу демілітаризовану зону, тобто фізично розділити DMZ, корпоративну та промислову мережі . Мережеві вузли, а саме сервер архівування та даних(HP ProLiant DL380 Gen9), до якого потрібно мати доступ як з корпоративної так і з промислової мережі інтегрований в DMZ.

В результаті обмін інформації між компонентами виглядатиме наступним чином(див рис. 4.3):

– Корпоративна мережа буде ініціювати зв'язок з DMZ ;
– Промислова мережа буде ініціювати зв'язок з DMZ.

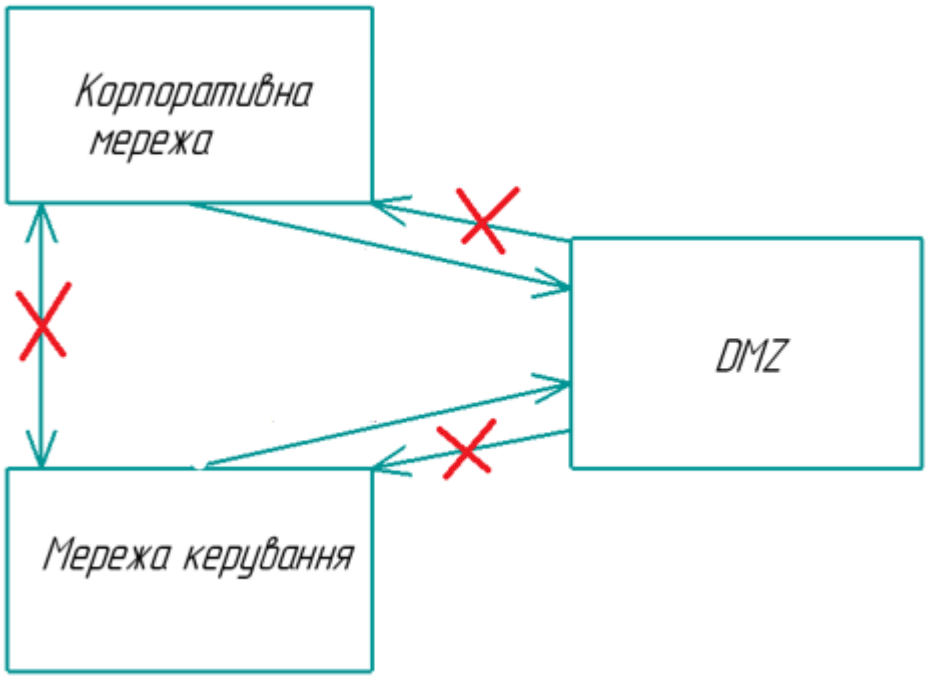


Рис. 4.3 Обмін даними між мережами

Перевагами такої архітектури є: гнучкість та незалежність від протоколу, зручна конфігурація та адміністрування, контрольоване розділення мереж, яка захищає чутливі корпоративні дані від несанкціонованого доступу, масштабована функціональність безпеки, дистанційна діагностика.

Створення даної архітектури потребує брандмауера, який підтримує мінімум три інтерфейси, один з який під'єднується до промислової мережі, інший до корпоративної а третій до DMZ. Необхідний безперервний контроль вихідного та вхідного мережевого трафіку в демілітаризованій зоні, також з'єднання з мережею керування повинні бути ініційовані пристроями мережі керування.

4.8.4 НАЛАШТУВАННЯ БРАНДМАУЕРА

Брандмауер – це мережевий пристрій безпеки, який контролює вхідни1 та вихідний мережевий трафіка вирішує чи дозволити чи блокувати певний трафік на основі визначених правил безпеки.[10]

Обраний брандмауер Siemens SCALANCE S623 має наступні функції безпеки:

1. Захист пристроїв або цілих доменів автоматизації з або без незалежний функцій безпеки інтегрованих брандмауером:

- перевірка IP пакетів на основі джерела та адреси призначення;
- підтримка Ethernet “non-IP” протоколів;
- обмеження пропускної здатності;
- загальні та локальні правила брандмауера;
- правила брандмауера визначені користувачем;
- введення журналу.

2. Режим маршрутизатора, в якому брандмауер відокремлює внутрішню мережу від мережі керування.
3. Встановлення безпечного зв’язку в незахищених мережах через VPN.

Наш брандмауер розташовується між корпоративною та промисловою мережами.

Налаштування брандмауера починається з правильного підключення мереж, червоний індикатор для корпоративної мережі, зелений для мережі керування, жовтий для DMZ.

Правила налаштування брандмауера наступні:

- Забороняти трафік за замовчуванням і дозволяти за винятком. Це гарантує нам, що будуть допускатись лишень затвердженні з’єднання(створення «білого списку»).
- Всі порти що не використовуються повинні бути відключені, щоб не створювати додаткових можливостей для підключення зловмисників. [1].
- Комунікація між корпоративною та демілітаризованою зоною повинен відбуватись по захищеному протоколу HTTPS, який в порівнянні HTTP має додаткове шифрування та аунтефікацію[6].
- Допускається лишень надсилання SMTP-повідомлень від мережі керування.
- Використання промислових протоколів дозволяється лишень всередині промислової мережі.
- Комунікації повинні здійснюватися тільки між зареєстрованими пристроями.

- Доступ до системи керування по можливості повинен бути ініційований пристроями системи керування.
- Всі комунікації з промисловою мережею повинні логуватися.

Для налаштування SCALANCE S623 спершу потрібно визначити модулі та їх IP адреси, отриманий результат занесемо в таблицю 4.1.

Таблиця 4.1 IP-адреси пристроїв

Мережа	Модуль	IP-адрес	Порт S623
Корпоративна мережа	ПК	172.158.2.6	172.158.2.2
Мережа керування	CP343-1Adv(комунікаційний процесор)	192.168.0.2	192.168.0.1
	ПК	192.168.0.3	
DMZ	Сервер	140.80.0.100	140.80.0.1

Першим кроком в конфігурації є створення нового проекту та користувача(адміна)(рис.4.4).

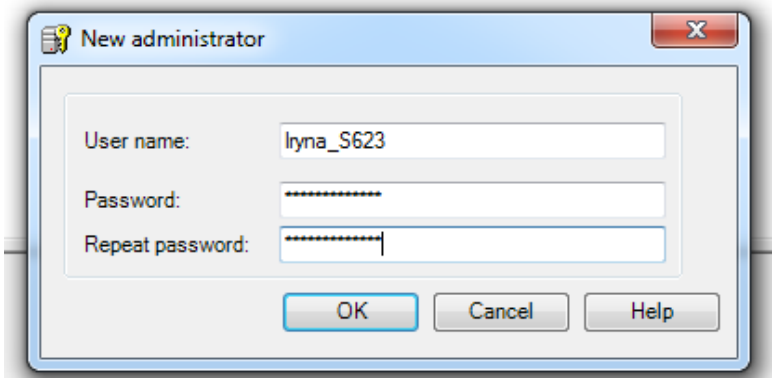


Рис.4.4 Створення нового адміністратора для конфігурації проекту

Наступним кроком є обрання модуля, в нашому випадку це S623, версія релізу повинна бути V3, так як використовується демілітаризована зона. Називаємо наш пристрій «DMZ», MAC address береться з задньої панелі, IP адреса корпоративної мережі присвоюємо IP адресі зовнішньої мережі, а IP адресу мережі керування – внутрішній мережі, для цього вибираємо режим роутер у брандмауера. Описані налаштування зображені на рис.4.5.

Рис.4.5 Програмна конфігурація брандмауера Siemens SCALANCE S623

Після цього для кожної з мереж потрібно прописати IP адреса портів(рис 4.6).

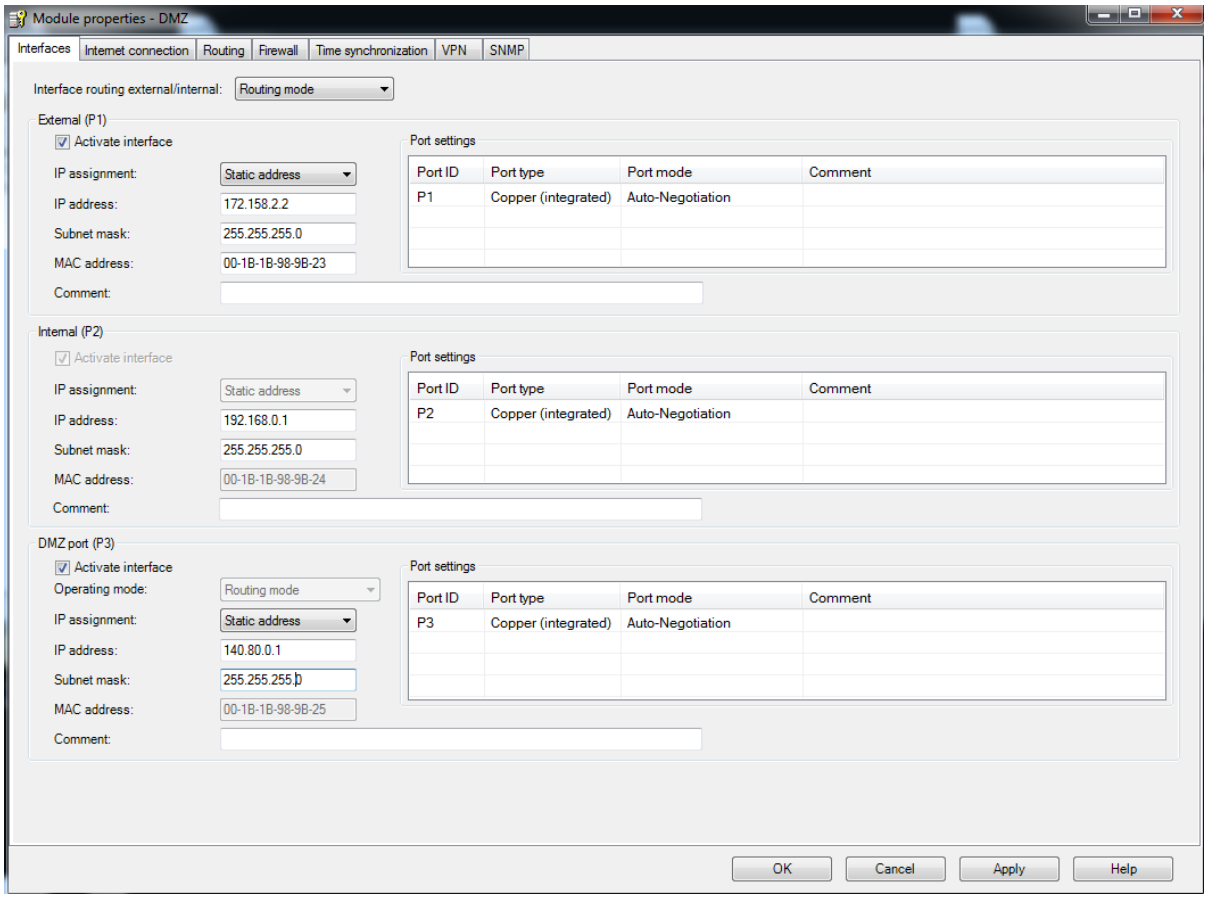


Рис 4.6 Налаштування портів пристою S623

Для конфігурації правил нам необхідно спершу прописати символьні змінні, які повинні містити короткий опис пристрою та його IP адрес(рис.4.7).

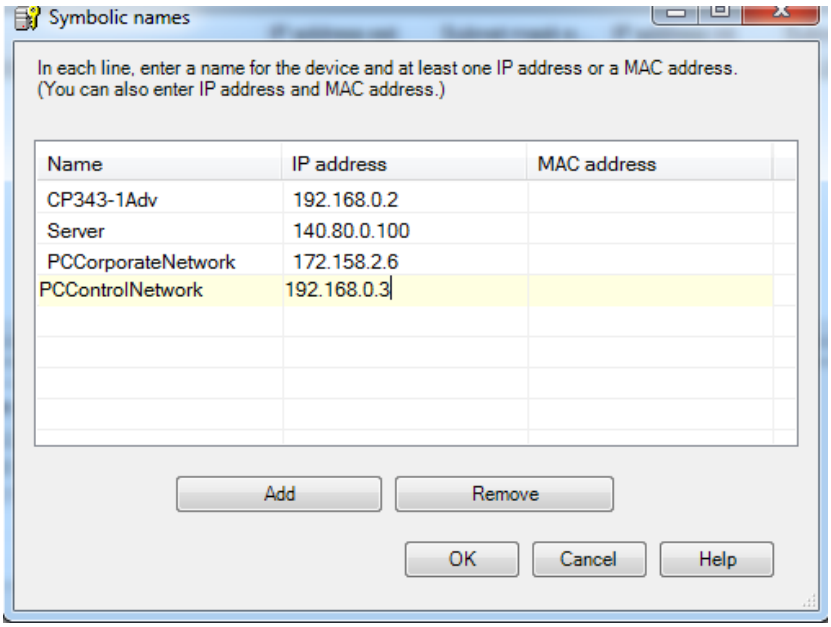


Рис 4.7 Символьні змінні пристрою S623

Дозволимо сервіс Syslog, який необхідний для комунікаційного сервера.(рис.4.8)

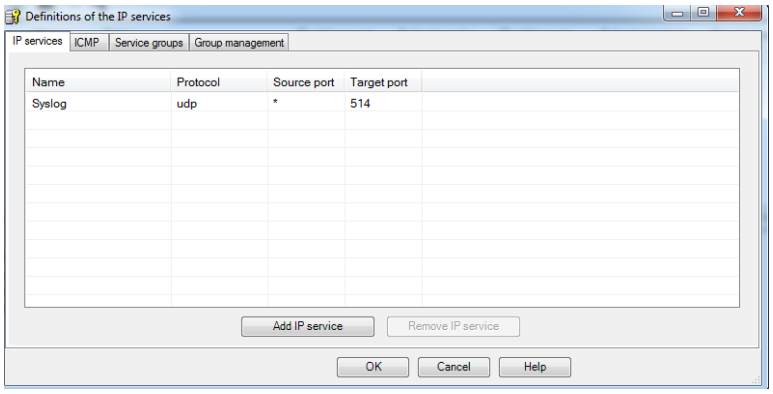


Рис.4.8 Сервіси пристрою

Відповідно до правил налаштування брандмауера та прийнятим обміном даними між мережами, прописуємо наступні IP-правила(рис.4.9), обираємо дозволені протоколи(рис.4.10) та вмикаємо логування пакетів(рис.4.11).

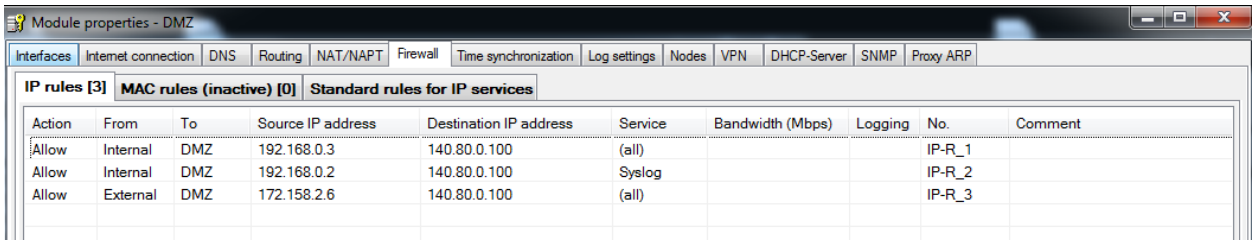


Рис.4.9 IP-правила налаштування брандмауера

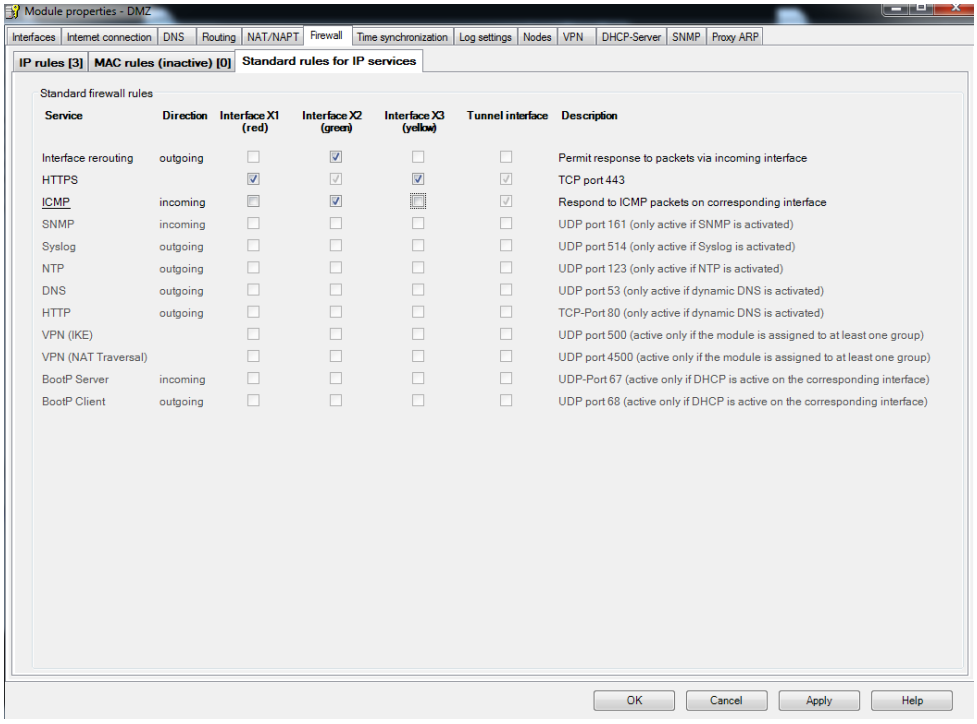


Рис 4.10 Стандартні правила для IP-сервісів брандмаувера

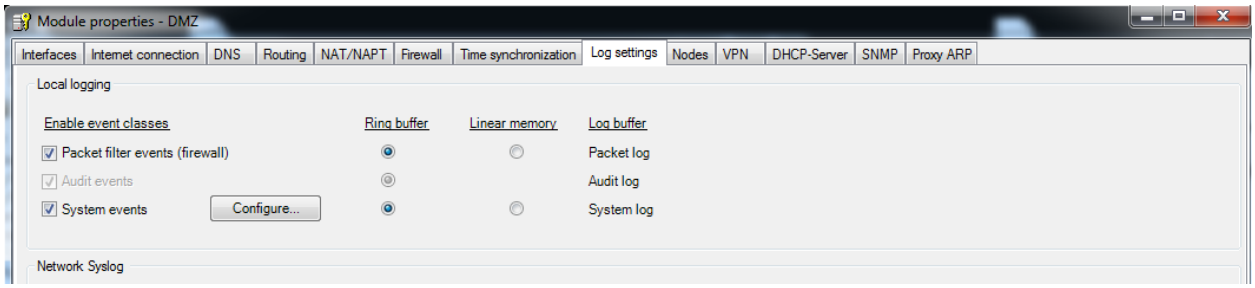


Рис.4.11 Налаштування логування пакетів у брандмауері

4.8.5 КЕРУВАННЯ ВІДДАЛЕНИМ ДОСТУПОМ

Критичним при конфігуруванні брандмауера є керування віддаленим доступом. Для нашої системи обрано модель керування доступом заснована на основі ролей. Дана модель є більш гнучкою у порівнянні зі списком контролю доступу.

Дана модель керуванням доступу полягає в тому, що ролі призначаються суб'єктам, внаслідок чого вони отримують дозволи через ролі. Завдяки цьому не виникає складно контрольованих відносин між суб'єктами і дозволами. Також внаслідок того що ролі можуть унаслідуватись, вони можуть містити дозволи надані не тільки конкретній ролі а й успадковані. Це спрощує систему адміністрування доступом[8].

4.8.6 АВТЕНТИФІКАЦІЯ ТА АВТОРИЗАЦІЯ

Автентифікація користувача або системи – це процес перевірки заявленої особи. Авторизація – це процес надання права доступу для користувача, визначається шляхом щодо правил ідентифікації та іншої відповідної інформацію[1].

На підприємстві «Таркетт-Вінісін» використовується центральна система автентифікації Microsoft Active Directory, яка є LDAP сумісна і використовується для зберігання всіх облікових записів та управління автентифікацією та авторизацією всіх осіб та систем.

Для доступу до SCADA- системи використовується SIMANTIC Logon для WinCC, який забезпечує такі функції як автоматичний вихід по тайм-ауту та

блокування облікового запису після багатократного неправильного вводу паролю. Також всі входи логуються в захищений журнал WinCC-Audit.

ВИСНОВКИ ДО РОЗДІЛУ 4

В даному розділі було проведено оцінку можливих кібер-загроз на систему керування котлом, шляхи покращення кібербезпеки системи керування котлом та процедуру реагування і виявлення кібератаки.

Було встановлено, що велику загрозу для кібербезпеки промислової мережі становить її спільний мережевий трафік з корпоративною мережею, в результаті чого було здійснено розшарування мереж, сервер архівування до якого вимагався спільний доступ було розміщено в демілітаризовану зону доступ до якої керується за допомогою брандмауера, який конфігурований у відповідності до правил наведених у 4.9.4. Такий підхід забезпечує обмеження в доступі до промислової мережі з боку корпоративної, у якій використовуються не завжди захищені протоколи обміну інформацією. Обрано інструменти для раннього виявлення кібератак, Wireshark та SolarWinds Server & Application Monitor, які дозволяють відстежувати поточний стан мережі. Визначено перелік команд з визначенням їхніх функцій, які беруть участь у процедурі відновлення та поетапні кроки реагування на кібератаку. Для керування доступом була обрана модель на основі ролей, за авторизацію та автентифікацію відповідає Microsoft Active Directory. Доступ до SCADA-системи реалізовується за допомогою SIMANTIC Logon.

5 РОЗРОБКА СТАРТАП-ПРОЕКТУ

Розробимо стартап-проект згідно до методичних вказівок [5].

5.1 ОПИС ІДЕЇ ПРОЕКТУ

Зміст ідеї, можливі напрямки застосування, основні вигоди, відмінність від аналогів наведено в таблиці 5.1.

Таблиця 5.1 Опис ідеї стартап-проекту

Зміст ідеї	**Напрямки застосування**	**Вигоди для користувача**
Організація кібербезпеки та впровадження розшарування мереж із застосуванням промислового брандмауера	Впровадження заходів кібербезпеки для вже існуючої системи автоматизації	Впровадження захисту від кібератак
	Модернізація існуючої системи з впровадженням заходів кібербезпеки системи керування	Оновлення застарілого обладнання та технологій більш сучасними та впровадження заходів кібербезпеки

Аналіз потенційних техніко-економічних переваг у порівнянні із пропозиціями конкурентів наведено в таблиці 5.2.

Таблиця 5.2 Визначення сильних, слабких та нейтральних характеристик ідеї проекту

№ п/п	Техніко-економічні характеристики ідеї	Концепції конкурентів			W (слабка сторона)	N (нейтральна сторона)	S (сильна сторона)
		Мій проект	Кригер	PELLETS HOME			
1	Організація кібербезпеки АСУ	Присутня	Відсутня	Відсутня			+
2	Надійність обладнання АСУ	Висока надійність обладнання	Середня ступінь надійності обладнання	Середня ступінь надійності обладнання			+
3	Вартість	Вище середньої	Середня	Нижче середньої	-		

5.2 ТЕХНОЛОГІЧНИЙ АУДИТ ІДЕЇ ПРОЕКТУ

Технологічний аудит ідеї наведено в таблиці 5.3.

Таблиця 5.3 Технологічна здійсненність ідеї проекту

№ п/п	Ідея проекту	Технології її реалізації	Наявність технології	Доступність технологій
1	Організація кібербезпеки АСУ	Брандмауер, аналізатор трафіку мережі та протоколу, моніторинг продуктивності мережі, система виявлення вторгнень	Технологія наявна	Широкий доступ до технології
Обрана технологія реалізації ідеї проекту: реалізація автоматичного керування буде здійснюватися за допомогою ПЛК; реалізація супервізорного рівня буде відбуватись за допомогою SCADA-системи; реалізація захисту від кібератак буде відбуватись за допомогою використання брандмауерів аналізатору трафіку мережі та протоколу, моніторингу продуктивності мережі, системі виявлення вторгнень та організаційних рішень на підприємстві.				

Отриманий результат свідчить про те що ідея проекту є технологічно можливою.

5.3 АНАЛІЗ РИНКОВИХ МОЖЛИВОСТЕЙ ЗАПУСКУ СТАРТАП-ПРОЕКТУ

Аналіз попиту наведений в таблиці 5.4.

Таблиця 5.4 Попередня характеристика потенційного ринку стартап-проекту

№ п/п	Показники стану ринку	Характериска
1	Кількість головних гравців, од	3
3	Динаміка ринку	Зростає
4	Наявність обмежень для входу	Немає
5	Специфічні вимоги до стандартизації та сертифікації	Немає
6	Середня норма рентабельності в галузі	15.5%

В результаті можна зробити висновок, що так як спостерігаються зростаюча динаміка ринку, кількість гравців не велика та середня норма рентабельності перевищує банківський відсоток то проект є рентабельним.

Потенційні групи клієнтів наведені в таблиці 5.5

Таблиця 5.5 Характеристика потенційних клієнтів стартап-проекту

№ п/п	Потреба, що формує ринок	Цільова аудиторія	Відмінності у поведінці потенційних цільових груп клієнтів	Вимоги споживачів до товару
1	Збільшення кількості кібератак на промислові об’єкти	Промислові підприємства, затримка і втручання в роботу яких, може призвести до великих збитків та серйозних наслідків	Відмінності у вартості та цільового призначення продукту	Система повинна забезпечувати обмеження в доступі системи керування до відкритих мереж, впровадити організаційні моменти та систему виявлення вторгнень

Аналіз ринкового середовища наведений в таблицях 5.6, 5.7.

Таблиця 5.6 Фактори загроз

№ п/п	Фактор	Зміст загрози	Можлива реакція компанії
1	Висока вартість системи	Споживачі не завжди готові витрачати кошти на ймовірні загрози, які можуть і не виникнути	Проведення інформування клієнтів, розробка оцінки ризиків
2	Нехтування кібербезпекою на підприємствах	Використання відкритих протоколів обміну даними та поєднання корпоративної та мережі керування, спрощує менеджмент підприємства	Проведення розшарування мережі підприємства та створення демілітаризованої зони з доступом до неї через брандмауер, дозволить залишити обмін даними між корпоративною та мережею керування,

Таблиця 5.7 Фактори можливостей

№ п/п	Фактор	Зміст загрози	Можлива реакція компанії
1	Збільшення кількості кібератак на промислові підприємства	Організація кібербезпеки системи керування	Проведення інформування щодо можливих наслідки кібератаки без впровадження кібербезпеки системи керування

Аналіз пропозиції наведено в таблиці 5.8.

Таблиця 5.8 Ступеневий аналіз конкуренції на ринку

Особливості конкурентного середовища	В чому проявляється дана характеристика	Вплив на діяльність підприємства
Тип конкуренції - чиста	Жоден із учасників не впливає на загальну ситуацію на ринку	Участь у відкритих тендерах, реклама на ринку, використання сучасних технологій
Рівень конкурентної боротьби – національний	Впровадження проекту потребує залучення майже всієї команди, що знижує мобільність та перешкоджає виходу на інтернаціональний ринок	Інформування та пошук нових клієнтів на території всієї держави
Конкуренція за галузевою ознакою - внутрішньогалузева	Інші галузі не мають аналогічних пропозицій та можливостей для повного забезпечення потреб клієнта	Пропонувати клієнтам продукт орієнтований на їхні особливі потреби
Конкуренція за видами товарів- товарно видова	Конкуренція з іншими пропонованими системами автоматичного управління	Використання сучасних технологій та надійного обладнання
Конкуренція за видами конкурентних переваг – цінова	Залежить від вартості	Оптимізація вартості проекту, в порівнянні з конкурентними пропозиціями
Конкуренція за інтенсивністю – марочна	Існують аналогічні пропозиції	Пропозиція відмінних від конкурентів

Після проведення аналізу конкуренції, проведемо детальніший аналіз умов конкуренції в галузі за моделлю 5 сил М. Портера. Отриманий результат наведемо в таблиці 5.9

Таблиця 5.9 Аналіз конкуренції в галузі за М. Портером

Складові аналізу	Прямі конкуренти в галузі	Потенційні конкуренти	Постачальники	Клієнти	Товари замінники
	Кригер	Низький бар'єр входження в ринок	Зміна ціни та мінімальна кількість замовлення	Контроль за якістю виконання	Немає
Висновки	Низька інтенсивність конкурентної боротьби	Існує можливість входу на ринок, через малу кількість конкурентів	Постачальники можуть диктувати умови на ринку, вартість обладнання	Клієнти диктують свої умови на ринку згідно до технічного завдання	Товари замінники відсутні

Визначення та обґрунтування факторів конкурентоспроможності наведено в таблиці 5.10.

Таблиця 5.10 Обґрунтування факторів конкурентоспроможності

№ п/п	Фактор конкурентоспроможності	Обґрунтування
1	Впровадження та організація кібербезпеки АСУ	Відсутність кібербезпеки системи керування у порівнянні з конкурентами

Аналіз сильних й слабких сторін стартап-проекту наведено в таблиці 5.11.

Таблиці 5.11 Порівняльний аналіз сильних та слабких сторін проекту

№ п/п	Фактор конкурентоспроможності	Бали 1-20	Рейтинг товарів-конкурентів у порівнянні з конкурентами						
			-1	-2	-3	0	+1	+2	+3
1	Кібербезпека системи керування	20	+						
2	Надійність обладнання та системи	18		+					
3	Вартість	14					+		

Завершальний етап ринкового аналізу можливості впровадження проекту є SWOT-аналіз(табл. 5.12) на основі виділених ринкових можливостей та загроз, слабких та сильних сторін наведених вище в таблиці 5.11.

Таблиця 5.12 SWOT-аналіз стартап-проекту

Сильні сторони: Наявність кібербезпеки в створеній системі	Слабкі сторони: Вартість
Можливості: Розуміння важливості впровадження кібербезпеки для систем автоматизації	Загрози: Поява схожих пропозицій на ринку

Розробимо альтернативи ринкової поведінки беручи за основу SWOT-аналіз. Альтернативи наведені в таблиці 5.13.

Таблиця 5.13 Альтернативи ринкового впровадження стартап-проекту

№ п/п	Альтернатива	Ймовірність отримання ресурсів	Строки реалізації
1	Орієнтація проекту на державні підприємства	70%	4 міс.
2	Орієнтація проекту на великі промислові підприємства	65%	8міс.
3	Орієнтація на іноземні підприємства	40%	4 міс.

З наведених вище альтернатив орієнтація проекту на державні підприємства дає вищу ймовірність отримання ресурсів та невеликий термін реалізації, тож обираємо дану альтернативу.

5.4 РОЗРОБКА РИНКОВОЇ СТРАТЕГІЇ ПРОЕКТУ

Насамперед для розробки ринкової стратегії визначимо охоплення ринку, отриманий результат занесемо в таблицю 5.14.

Таблиця 5.14 Вибір цільових груп потенційних споживачів

№ п/п	Опис профілю цільової групи потенційних клієнтів	Готовність споживачів прийняти продукт	Орієнтований попит в мажах цільової групи	Інтенсивність конкуренції в сегменті	Простота входу в сегмент
1	Власники підприємств втручання в роботу яких несе за собою великі фінансові збитки	Готовий прийняти продукт	Високий	Низка	Просто
2	Власники великих промислових підприємств	Потребує додаткового переконання в користі продукту	Середній	Низька	Просто
Які цільові групи обрано: Власники підприємств втручання в роботу яких несе за собою великі фінансові збитки					

Відповідно до цільових груп найкращим чином буде застосування стратегії диференціального маркетингу, що має на увазі роботу з декількома сегментами на ринку.

Для обраної цільової аудиторії сформуємо базову стратегію розвитку(табл. 5.15).

Таблиця 5.15 Визначення базової стратегії розвитку

№ п/п	Обрана альтернатива розвитку	Стратегія охоплення ринку	Ключові конкурентоспроможні позиції відповідно до обраної альтернативи	Базова стратегія розвитку
1	Орієнтація проекту на державні підприємства	Диференціальний маркетинг	Великі помислові підприємства мають більшу потребу в кіберзахисті	Диференціації

Таблиця 5.16 Визначення базової стратегії конкурентної поведінки

№ п/п	Чи є проект «першопроходцем» на ринку?	Чи буде компанія шукати нових споживачів, або забирати в існуючих конкурентів	Чи буде компанія копіювати основні характеристика товару конкурента і які?	Стратегія конкурентної поведінки
	Ні	Буде шукати нових споживачів	Буде копіювати характеристики товару, які забезпечать покращення проекту	Стратегія заняття конкурентної ніші

На основі таблиць 5.5 та 5.15 розробимо стратегію позиціонування отриманий результат занесемо в таблицю 5.17.

Таблиця 5.17 Визначення стратегії позиціонування

№ п/п	Вимоги до товару цільової аудиторії	Базова стратегія розвитку	Ключові конкурентоспроможні позиції проекту	Вибір асоціацій, які мають сформувати комплексну позицію проекту
1	Захист системи керування від кібератак	Стратегія диференціації	Впровадження та організація кібербезпеки, надійність обладнання, адаптація проекту під кожного споживача	Система автоматичного керування, захист інформації в системах керування

В результаті даного розвитку ми отримали узгоджену систему рішень ринкової поведінки.

5.5 РОЗРОБКА МАРКЕТИНГОВОЇ ПРОГРАМИ СТАРТАП- ПРОЕКТУ

Насамперед потрібно сформувати маркетингову концепцію товару, для цього підсумуємо результати попереднього аналізу конкурентоспроможності(табл. 5.18).

Таблиця 5.18 Визначення ключових переваг концепції потенційного товару

№ п/п	Потреба	Вигода, яку пропонує товар	Ключові преваги перед конкурентами
1	Захист та організація кібербезпеки на підприємстві	Впровадження та організація кібербезпеки системи керування	Відсутність забезпечення потреби в конкурентів

Тепер визначимо цінові межі, на які будемо орієнтуватись при встановленні ціни, результати занесемо в таблицю 5.19

Таблиця 5.19 Визначення меж встановлення ціни

№ п/п	Рівень цін на товари-замінники	Рівень цін на товари-аналоги	Рівень доходів цільової групи споживачів	Верхня та нижня межа встановлення ціни а продукт
1	400000-700000	500000-800000	300000-5000000	2000000-700000

Проведемо визначення оптимальної системи збуту, результат занесемо в таблицю 5.20

Таблиця 5.20 Формування системи збуту

№ п/п	Специфіка закупівельної поведінки цільових клієнтів	Функції збуту, які має виконувати постачальник товару	Глибина каналу збуту	Оптимальне система збуту
1	тендери	Вчасна поставка та дотримання домовленостей	Спілкування на пряму з клієнтами	Проведення збуту шляхом брання участі в тендерах

Останньою складовою є розроблення концепції маркетингових комунікацій, результат занесемо в таблицю 5.21.

Таблиця 5.21 Концепція маркетингових комунікацій

№ п/п	Специфіка поведінки цільових клієнтів	Комунікаційні канали, якими користуються цільові клієнти	Ключові позиції, обрані для позиціювання	Завдання рекламного повідомлення	Концепція рекламного звернення
1	Тендери для оцінки всіх пропозицій	Рекомендації, телефон, веб-сайти	Система автоматичного керування, захист інформації в системах керування	Пропаганда впровадження кібербезпеки в системах керування	Демонстрація функціоналу

ВИНОВКИ ДО РОЗДІЛУ 5

В даному розділі було проведено технічний аудит системи , в результаті якого проект зробили висновок, що його технологічно можливо реалізувати. Також проведено аналіз ринкових можливостей, розробку ринкової та маркетингової стратегії. Отриманий результат свідчить, що проект можу бути технологічно реалізований, він має переваги в порівнянні з конкурентами, та існує невелика кількість конкурентів, просто зайти на ринок.

ВИСНОВКИ

Підчас виконання магістерської дисертації було автоматизовано процесу горіння в твердопаливному котлі та організовано кібербезпеку системи керування, а саме:

1. Вивчили принцип та особливості роботи твердопаливного котла, навели короткий опис та технологічні параметри.

2. Для вибраних контурів регулювання: теплового навантаження, вмісту кисню у вихідних газах, розрідження в топці було розраховано регулятори трьома методами, РАФХ та два експрес методи та розраховано показники якості за якими обрано більш оптимальний процес, який забезпечує невеликий час регулювання та перерегулювання.

3. Розроблено програмне забезпечення супевізорного та локального рівняв ПТКЗА. Основою даної системи є Siemens Simatic S7-300. Локальний рівень містить програмне забезпечення для контролера. Супервізорний рівень забезпечує можливість ручного керування, моніторинг технологічних параметрів, можливість зміни уставки, регулюючого впливу, відображає аварії, які виникають та тренди регульованих технологічних параметрів.

4. Проведено оцінку можливих кібер-загроз на систему керування котлом, шляхи покращення кібербезпеки системи керування котлом та процедуру реагування і виявлення кібератаки. Здійснено розшарування мереж, який забезпечує обмеження в доступі до промислової мережі з боку корпоративної. Обрано інструменти для раннього виявлення кібератак, Wireshark та SolarWinds Server & Application Monitor. Визначено перелік команд з визначенням їхніх функцій, які беруть участь у процедурі відновлення та поетапні кроки реагування на кібератаку. Керування доступом здійснюватиметься за допомогою модель на основі ролей. Доступ до SCADA-системи реалізовується за допомогою SIMANTIC Logon.

5. Розроблено стартап-проект для системи керування процесом горіння та організації кібербезпеки цієї системи. Згідно до розробленого проекту проект технічно можна реалізувати. В результаті оцінки ринку та конкурентів

визначили, що просто зайти на ринок, через відсутність великої кількості конкурентів. Обрали стратегію диференціального маркетингу для охоплення ринку, а стратегію розвитку – диференціації.

В результаті виконання даної роботи отримали автоматизовану систему керування твердопаливним котлом та організацію кібербезпеки, яка готова до впровадження на підприємства.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ackerman P. Industrial Cybersecurity. Birmingam, 2017. 515p.
2. ISA-62443[multiple parts], Security for Industrial Automation and Control Systems, Research Triangle Park, North Carolina: International Society of Automation, 2009.
3. National Institute of Standards and Technology Special Publication (USA) 800-82 Revision 2. Guide to Industrial Control Systems (ICS) Security. [Electronic Resource] / Stouffer K., Pillitteri V., Lightman S., Abrams M. Hahn., 2005, 247p.
4. Довідковий посібник з комплексного інженерного розрахунку промислових АСР в курсовому і дипломному проектуванні із спеціальностей "АТПіВ", "КІТПіВ".
5. Розроблення стартап-проекту [Електронний ресурс] : Методичні рекомендації до виконання розділу магістерських дисертацій для студентів інженерних спеціальностей / За заг. ред. О.А. Гавриша. – Київ : НТУУ «КПІ», 2016. – 28 с.
6. Foremski “Mutrics: Multilevel traffic classification” [Електронний ресурс]. – Режим доступу: http://mutrics.iitis.pl/
7. O’Dwyer A. Handbook of PI and PID Controller. Tuning Rules. 3rd Edition. London, 2009. 623p.
8. Osborn S., Sandhu R., and Nunawer Q. Configuring Role-Based Access Control To Enforce Mandatory And Discretionary Access Control Policies. ACM Trans. Info. Syst. Security, 2000.
9. Технологічний регламент виробництва напівфабрикату паркетного покриття / Укл. Бенець Т.П.-К.: "Tarkett.ua".2014.-94с.

УДК 004.72
Магістрант 5 курсу, гр. ТО-81мп Яремчук І.Т.
Доц., к.ф.-м.н. Бобков В.Б.

ІНТЕГРАЦІЯ МОДУЛІВ ІІОТ З СИСТЕМАМИ ВЕРХНЬОГО РІВНЯ

Одним з сучасних трендів розвитку інформаційних технологій є промисловий інтернет речей ІІоТ. Окрім вирішення задач неперервного моніторингу показників роботи обладнання зібрані та оброблені дані можуть використовуватись для модулів ERP-систем при прийнятті рішень щодо управління виробництвом. Приклади подібного підходу продемонстровані та впроваджені вітчизняною компанією IT-Enterprise, яка вважається одним лідерів напрямку Industry 4.0 в Україні. Компанією розроблено модуль ІІоТ на базі вільно розповсюджуваного фреймворку Node Red. Створено адаптери для основних промислових протоколів обміну даними та реалізовано інтеграцію з верхнім рівнем. Реалізовано наступні рішення:

- Аналіз простоїв на основі обробки показників датчиків, встановлених на обладнанні, що базується на критеріях, реалізованих у вигляді правил в модулі ІІоТ
- Завантаження програм в верстати з ЧПУ на основі планування, яке здійснюється в ERP-модулях
- Планування ремонтів на основі обробки показників датчиків обладнання

Отже можливі дві схеми інтеграції. Перша полягає в налаштуванні модуля ІІоТ для збирання даних за певним протоколом, конфігуруванні алгоритму агрегації показників з передачею агрегованих даних на верхній рівень та подальшим їх аналізом в ERP-модулях. Друга схема (Рис.1) реалізує зворотній напрямок руху даних – на основі планування, що здійснюється в модулі верхнього рівня, відбувається управління обладнанням через модуль ІІоТ.

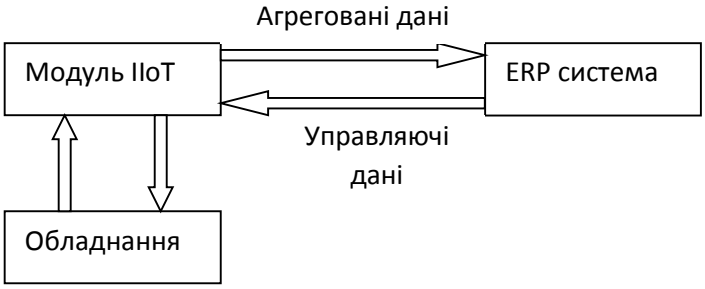


Рис.1 Схема інтеграції з модулем ІІоТ

Описаний підхід дозволяє досягти автоматизації на всіх рівнях. Зокрема, використовуючи новий продукт для житлово-комунального господарства від компанії IT-Enterprise, можна реалізувати облік споживання електроенергії, інтегруючи цей продукт з лічильниками. На верхньому рівні можна реалізувати також оптимізацію енергоспоживання на основі обробки даних, переданих з модуля ІІоТ. В даній роботі демонструється подібне рішення на основі обладнання учбової лабораторії.

Перелік посилань:

1. Li, X., Lu, R.X., Liang, X.H., Shen, X.M., Chen, J.M., Lin, X.D. Smart community: An Internet of Things application, IEEE Communications Magazine vol. 49, pp. 68, 75, 2011.

УДК 004.9

Магістрант 5 курсу, гр. ТО-81мп Яремчук І.Т.
Ст.викл. Грудзинський Ю.Є.

АНАЛІЗ РІВНЯ БЕЗПЕКИ І РИЗИКУ ПРИ СТВОРЕННІ СИСТЕМ "РОЗУМНИЙ БУДИНОК"

По мірі зростання добробуту та поширення технологічних гаджетів ми полегшуємо собі повсякденне життя, автоматизуючи тривіальні і нагальні задачі. Все більше впровадження систем розумного будинку (SHS) приводить нас до необхідності організації безпечного, надійного і функціонального середовища.

Проблема ще більш ускладнюється із-за того, що частина зібраних даних від датчиків буде передаватися потенційно небезпечною мережею Інтернет до хмарних сервісів. Тому при створенні SHS вкрай важливо виконати умови як безпеки, так і конфіденційності.

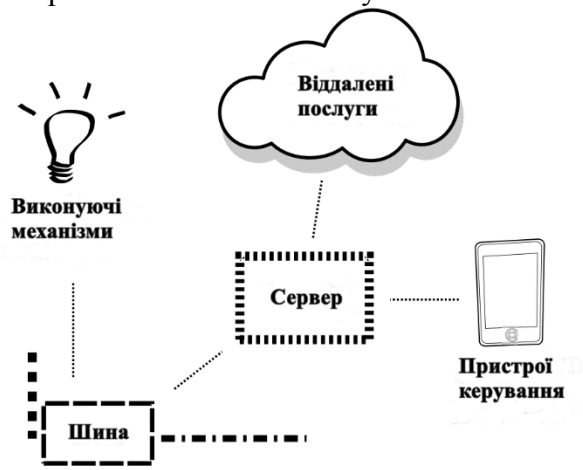


Рис 1. П’ять категорій ризику

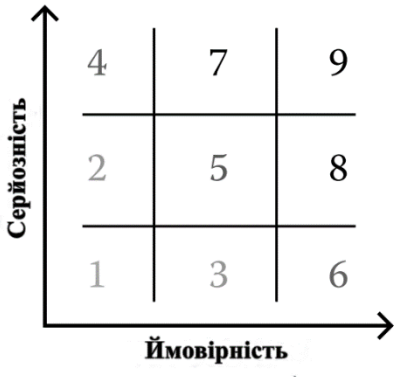


Рис 2. Дев’ять категорій ризику

У нашому досліджені згруповані можливі вектори атак SHS за п'ятьма категоріями вразливостей: (1) сервер для управління станом і для надання інтерфейсу управління або API, (2) шину для зв'язку з пристроями і (3) пристрої – виконуючі механізми. Вся ця система керується користувачем зі свого смартфона (4). Крім того, користувачем можуть бути додатково укладені договори зі сторонніми службами для розширення основних функцій системи (5). Всі ці п'ять категорій вразливостей повинні бути розглянуті на етапі розробки SHS. Категорії і їх комунікативна взаємодія представлено на рис. 1.

Для подальшого аналізу самі атаки розподілено на дев'ять категорій відносного і передбачуваного ризику: низький, середній і високий по кожному з двох вимірів: серйозність і ймовірність так, як показано на рис. 2. Поняття ризику засноване на тому, наскільки ймовірна і наскільки серйозна ця атака. При аналізі відзначаємо, що більш імовірним атакам присвоюються вищі рейтинги ризику, ніж більш серйозним.

Перелік посилань:

1. Li, X., Lu, R.X., Liang, X.H., Shen, X.M., Chen, J.M., Lin, X.D. Smart community: An Internet of Things application, IEEE Communications Magazine vol. 49, pp. 68, 75, 2011.
2. Eom, B., Lee, C., Yoon, C., Lee, H., Ryu, W. A platform as a service for smart home, International Journal of Future Computer and Communication vol. 2, no. 3, pp. 253, 257, 2013.
3. Cook, D. How smart is your home? Science vol. 335, no. 6076, pp. 1579,1581, March 2012.

Технічні науки

Грудзинський Ю.Є., к.т.н. Бунь В.П., Яремчук І.Т.

Національний технічний університет України "Київський Політехнічний Інститут імені Ігоря Сікорського", Україна

СМАРТФОН, ЯК ЗАСІБ КІБЕРАТАКИ

Аннотація

У сьогоднішньому технологічному світі, що швидко розвивається, мобільні обчислювальні пристрої піддаються підвищеному ризику нападу при експлуатації. Проблеми безпеки мобільних пристроїв включають загрози, такі як фізична крадіжка або випадкова втрата пристрою, зловмисне програмне забезпечення для мобільних пристроїв, несанкціонований доступ, шахрайство на основі мобільного зв'язку, шпигунство та багато іншого. Тут телефонні дзвінки, SMS, Bluetooth і доступ до Інтернету діють як потенційні канали загрози безпеки пристрою смартфона. У цій статі класифікуються різні типи та деталі загроз кібербезпеки пристрою смартфона. Наводиться вичерпний перелік простих і дешевих профілактичних заходів, які можуть бути використані користувачем для підвищення безпеки мобільних пристроїв і і захищенності даних.

Ключові слова: смартфон, мобільний пристрій, мобільні обчислення, загрози, ризики.

Вступ

Завдяки мобільності та універсальності наявних застосунків, смартфони та планшети швидко стають кращими інструментами для перегляду інтернет-сторінок, онлайн-транзакцій, аукціонів, покупок, віддаленого керування пристроями. Еволюція смартфонів проклала процвітаючий шлях для зростання громадянського суспільства, але вона також відкрила можливості для кіберзлочинців використовувати мобільні пристрої в якості каналу або засобу атаки як персональних даних користувачів, так і різноманітних пристроїв в IoT.

Вразливості мобільних обчислювальних інфраструктур існують в самому апаратному забезпеченні пристроїв, архітектурі застосунків, стандартах кодування, бездротовому підключенні і навіть у протоколах передачі даних. Такі вразливості завжди піддають ризику як гроші саміх користувачів, так і безпеку роботи пов'язаних пристроїв IoT. Низькі ціни, портативність і величезний обчислювальний потенціал сучасних мобільних пристроїв роблять їх кращим

інструментом для виконання злочинних дій [1]. Тому актуальним є виявлення та публікація простих та доступних дій користувача, котрі дають змогу значно зменшити ці ризики.

Постановка питання

Діяльність, пов'язану з незаконним використанням мобільних телефонів можна розглядати як мобільні злочини. Така діяльність використовує один або декілька потенційних видів мобільних пристроїв для вчинення злочинів. Тут ми обговоримо різні види мобільних злочинів.

Фізична крадіжка: легкість перенесення мобільних пристроїв робить їх дуже вразливими до фізичних крадіжок. Злочинці можуть виставляти привабливу ціну за вкрадені мобільні пристрої на чорному ринку для дорогого обладнанню. Але для користувача, який є жертвою мобільної крадіжки або фізичної втрати, збитки поширюється і на втрату важливої та конфіденційної інформації, що зберігалася на пристрої [2]. Сучасні мобільні пристрої обладнані парольним захистом на основі символьних послідовностей, біометричним захистом [3], шифруванням даних користувача та механізмами стирання цих даних для мінімізації втрати інформації.

Рис. 0.1 Різноманітність злочинів пов’язаних з мобільними телефонами

Мобільне хакерство: будь-яке незаконне вторгнення в обчислювальний пристрій і/або мережу без згоди його власника, дії, що порушують безпеку мобільних пристроїв, систем зв'язку та мереж [4]. Для реалізації мобільного

злому хакери використовують навмисно написані сценарії або шкідливі програми, для націлювання на мобільні пристрої та системи, підключені до них.

Мобільний кібернаклеп: передача або трансляція навмисно написаної зневажливої, принизливої та непристойної інформації, образливої для репутації особи або організації, що викликає моральні, фізичні та/або фінансові втрати, називається наклепом [4].

Мобільна порнографія: порнографія вважається злочином у багатьох країнах. Після появи Інтернету та комп'ютерних технологій розповсюдження порнографії зробило величезний стрибок. Використання мобільних пристроїв, систем зв'язку, Інтернету та мобільних послуг для створення та передачі порнографії класифікується як мобільна порнографія [5, 6].

Крадіжка особистих даних: інформація про користувачів, розмови по електронній пошті, SMS-повідомлення, телефонні контакти, журнали викликів і історія перегляду, зазвичай зберігаються на мобільних пристроях. Крім того, ці пристрої також зберігають та передають конфіденційну інформацію, таку як фінансову та медичну, тощо.

Мобільне клонування: передача конфіденційних даних з одного телефону на інший, щоб зробити його точною копією оригінального телефону. Після клонування дзвінками та повідомленями можуть одночасно обмінюватися обидва телефони, тоді як лише тільки власник оригінального телефону оплачує всі дії клонованого телефону. Для клонування телефону CDMA, пара ESN/MIN у мікросхемі EPROM повинна бути скопійована у мікросхему EPROM іншого телефону CDMA. У випадку GSM-телефонів, достатньо копіювання оригінальної SIM-картки на іншу SIM-карту щоб завершити процедуру клонування [4, 7].

Мобільне переслідування: постійні та неодноразові акти погроз і переслідувань, спрямовані на життя, імідж та власність жертви, підпадають під цей термін.

Атака відмови в обслуговуванні: атака DDoS - це інший тип кібератаки, спрямований на затоплення обчислювальних ресурсів жертви фальшивими або

фіктивними запитами для порушення роботи звичайних послуг. Використання мобільних пристроїв, щоб затопити поштову скриньку жертви, папку вхідних SMS-повідомлень або пам'ять телефону, позбавляючи їх можливості нормальної роботи, можна класифікувати як мобільну атаку DDoS.

Піратство мобільного програмного забезпечення: незаконне копіювання, підробка або розповсюдження автентичних і захищених авторським правом мобільних програмних продуктів з наміром підробити або пошкодити оригінальне програмне забезпечення.

Поширення шкідливого програмного забезпечення: після ери шкідливих програм призначених для настільних компютерів та ноутбуків, нові програмні шкідники постійно розвиваються разом з вдосконаленням архітектур мобільних пристроїв. Шкідливе програмне забезпечення включає до себе троянів, хробаків, віруси, здирників і шпигунів.

Мобільний фішинг: клас атак на основі соціальної інженерії, які обманюють користувачів мобільних пристроїв, що стали жертвою зловмисних атак. Фішингові атаки можуть обманювати мобільного користувача-жертву, щоб ті самі передавали свої дані, фінансову інформацію, дані облікових записів, історію перегляду або завантажували шкідливе програмне забезпечення на свій мобільний пристрій.

Мобільне шпигунство: - означає прихований моніторинг окремих осіб або груп для отримання конфіденційних даних без їхньої згоди. Сучасні мобільні пристрої володіють великими обчислювальними можливостями, величезними банками пам'яті, GPS-спостереженням за пересуванням, гарною роздільною здатністю камери і аксесуарами, наприклад, мікрофоном.

Результати

Зменшення ризиків від фізичної втрати або крадіжки мобільного пристрою

Фізична втрата пристрою внаслідок крадіжки або втрати є серйозною загрозою для безпеки, оскільки на додаток до фінансової шкоди, користувач також втрачає повний фізичний контроль над своїми даними. Що стосується

людської природи та випадкових можливостей, то таких фізичних втрат, звісно, не можна гарантовано уникнути, але їх вплив можна знизити до мінімуму, якщо користувачі будуть виконувати наступні дії:

1. **Перевірка та застосування усіх можливих функцій безпеки, що надаються постачальником послуг мобільного зв'язку**: для кращого використання цих функцій безпеки краще використовувати унікальні комбінації паролів і випадкових питань безпеки, які не мають зв'язку з профілем соціальних мереж користувача.
2. **Не зберігати критично важливу інформацію на мобільному пристрої**: конфіденційні дані, такі як паролі облікових записів, PIN-коди, фінансові дані тощо. Особливо великому ризику втрати або крадіжки вони піддаються, якщо зберігаються в текстових повідомленях або електронних листах. Про крадіжку або втрату мобільного пристрою повинен бути негайно поінформований постачальник послуг, щоби якомога швидше віддалено вимкнути пристрій. Після цього користувач повинен змінити паролі всіх підключених онлайн-облікових записів, доступних через вкрадений пристрій.
3. **Встановлення достатньо сильних паролів доступу**: у випадку крадіжки або втрати, надійний пароль захищає дані користувача на досить задовільному рівні. Відсутність будь-якого пароля або знання цього пароля багатьма людьми в значній мірі загрожують захисту даних, що знаходяться на пристрої.
4. **Регулярне резервне копіювання**: користувачі мобільних пристроїв повинні регулярно створювати резервні копії даних, що зберігаються на їх пристроях, на додаткових пристроях зберігання даних, таких як зовнішні накопичувачі або карти пам'яті. Щоб підвищити рівень безпеки та доступність, можна зберігати ті ж дані у службах резервного копіювання у хмарному сховищі. Це дозволить користувачеві віддалено отримувати доступ, оновлювати та відновлювати свої дані з будь-якого місця в разі втрати, крадіжки або випадкового пошкодження пристрою.

5. **Правильне видалення даних перед переходом на новий пристрій**: перед тим як викинути, подарувати або навіть перепродати свій мобільний пристрій, необхідно виконати ефективне видалення даних зі старого пристрою, в цілях захисту своєї конфіденційності і безпеки. Для цього існують певні пристрої, а також програмні застосунки, які забезпечують задовільне видалення старих даних.
6. **Встановлення програмових застосунків для відстеження пристрою**: сучасні мобільні пристрої обладнанні функціями віддаленого відстеження, блокування та навіть видалення даних. Кілька невдалих спроб входу можуть призвести до самодеструкції усіх даних, що знаходяться на пристрої. Для надання таких функцій також доступно кілька програм.

Попередження фішінг-атак

Як було зазначено раніше, атаки фішінгу діють як приманка для мобільних користувачів, які є потенційними об'єктами для експлуатації кібер-злочинцями. Як правило, спроби фішінгу є атаками соціальної інженерії, вбудованими в текстові або телефонні формати викликів, щоб спонукати жертву наївно порушити безпеку свого пристрою. Але наступні заходи безпеки можуть значною мірою уберегти користувачів мобільних пристроїв від фішінг-атак.

1. **Ніколи не натискайте на підозріле посилання або номер**. При отриманні текстового повідомлення або телефонного дзвінка з підозрілим вмістом або з невідомого номера з проханням виконати певну дію, натиснувши посилання або набравши вказаний номер, - користувач ніколи не повинен виконувати запропоновані дії. Ця бездіяльність автоматично розброїть кинуту приманку віддаленого шахрая або кіберзлочинця.
2. **Підтвердьте обґрунтованість джерела**. При отриманні таких сумнівних повідомлень, цільовий користувач повинен завжди намагатися переконатись в його джерелі або відправнику. Пошук джерела може бути зроблено в пошукових системах або адресних каталогах через Інтернет.
3. **У разі самозванців, підтвердьте їхні повноваження**. Якщо сумнівне повідомлення або виклик надходять від одного з ваших відомих джерел, і в

них просять вас виконати певну дію, то краще звернутися безпосередньо до самого джерела, щоб підтвердити повідомлення.

4. **Ніколи не надавайте будь-яку особисту або конфіденційну інформацію у віддаленому режимі**. Обсяг особистої або конфіденційної інформації варіюється від фінансових даних до одноразових паролів, відомостей облікового запису користувача, навіть назви та адреси цільового користувача. Посилання фішінга зазвичай загрожують мобільним користувачам блокуванням конкретної послуги, наприклад, блокуванням кредитної картки. Користувачі повинні пам'ятати, що будь-які органи будь-якої законної служби ніколи не запитають про їхню конфіденційну інформацію. У разі сумніву користувачі повинні самі зразу звернутися до уповноваженого органу.

Попередження атак на основі програмових застосунків

1. **Завантажуйте лише з надійних платформ**: завжди завантажуйте мобільні застосування з надійних платформ, таких як «Google Play Store» для пристроїв Android чи «iTunes» для пристроїв Apple. Застосування, завантажені на ці платформи, ретельно перевірені та підтверджені. Програми, завантажені з невідомих або ненадійних платформ, можуть нести зловмисне або шпигунське програмне забезпечення, яке може піддати ризику безпеку даних на пристрої користувача.
2. **Вичерпно вивчіть усі особливості програми перед завантаженням**: оцінки, надані користувачами, історія та відгуки про авторів та історію оновлення програми. Таке вивчення повинно бути виконано перед встановленням будь-якого застосунка, навіть з найбільш надійних джерел, згаданих вище. Ця перевірка може врятувати користувача від будь-яких несподіваних втрат або збитків завданих програмою, якіх вже раніше зазнали інші користувачі.
3. **Перевірте дозволи програми перед встановленням**: користувач повинен вдумливо та обережно надавати новій програмі на її прохання дозволи доступу до даних і служб пристрою. Ця перевірка є надзвичайно важливою

для будь-якої програми, щоб дізнатися про її подальшу поведінку після встановлення на пристрої.

4. **Перевірка рахунку на телефоні**: у випадках ненормального обміну даними, раптового виснаження терміну служби батареї або незрозумілого нагрівання пристрою, перевірте ваш телефонний рахунок. Багато розповісти про підозрілі дзвінки або несподівані обміни текстовими повідомленнями може несподіване зменшення депозиту на рахунку.
5. **Встановіть програму безпеки.** Користувачі повинні встановити програму безпеки, яка сканує поведінку кожного застосунка, встановленого на пристрої. У випадку будь-яких програм-шпигунів або шкідливих програм, програма безпеки сповістить користувача про ненормальну поведінку такої програми.
6. **Використовуйте віртуальний номер для некритичного використання.** Це один з найкращих способів обмежити кількість особистої ідентифікації даних, прив'язаних до головного контактного номера. Використання віртуальних номерів для неособистісних питань може допомогти зберегти конфіденційність у багатьох випадках. Віртуальні номери можуть приймати текстові повідомлення та телефонні дзвінки, а також на них можна налаштовувати переадресацію на фактичний контактний номер, щоб уникнути втрат справжніх та важливих повідомлень.

Висновки

Сучасні технології мобільного зв'язку дозволили окремим особам та організаціям використовувати їх для спілкування в реальному часі та передачі даних у власних інтересах. Однак ця перевага одночасно пов’язана з ризиками кібербезпеки пов’язаних пристроїв і даних, якими вони керують. Щоб протистояти цим ризикам, необхідна ефективна політика управління, адекватна підготовка та всебічне знання про способи їх попередження. Ці принципи мають вирішальне значення для безпечного та безперебійного використання мобільних пристроїв. В цій статі зроблено спробу сформулювати ряд простих, недорогих

але ефективних дій користувача, направлених на зниження ризиків від використання мобільного пристрою.

Література

1. Burge, P., Shawe-Taylor, J., Cooke, C., Moreau, Y., Preneel, B., & Stoermann, C. (1997). Fraud detection and management in mobile telecommunications networks.
2. Badhe, A. (2016). Click Fraud Detection In Mobile Ads Served In Programmatic Exchanges. International Journal of Scientific Technology & Research, 5(4), 1.
3. Trewin, S., Swart, C., Koved, L., Martino, J., Singh, K., & Ben-David, S. (2012, December). Biometric authentication on a mobile device: a study of user effort, error and task disruption. In Proceedings of the 28th Annual Computer Security Applications Conference (pp. 159-168). ACM.
4. Barson, P., Field, S., Davey, N., McAskie, G., & Frank, R. (1996). The detection of fraud in mobile phone networks. Neural Network World, 6(4), 477-484
5. Badhe, A. (2016). Click Fraud Detection In Mobile Ads Served In Programmatic Exchanges. International Journal of Scientific Technology & Research, 5(4), 1.
6. Shawe-Taylor, J., Howker, K., & Burge, P. (1999). Detection of fraud in mobile telecommunications.
7. Information Security Technical Report, 4(1), 16-28.